I. J. Computer Network and Information Security, 2020, 6, 57-77
Published Online December 2020 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2020.06.05

A Proficient Mechanism for Cloud Security Supervision in Distributive Computing Environment

Kamta Nath Mishra
Department of Computer Science & Engg., Birla Institute of Technology, Mesra, Ranchi, INDIA
E-mail: mishrakn@yahoo.com

Received: 09 July 2020; Accepted: 13 September 2020; Published: 08 December 2020

Abstract: In the existing epoch, the cloud-IoT integrated distributive computing is earning very high attractiveness because of its immense characteristics which can be divided into two categories namely essential and common characteristics. The essential characteristics of cloud-IoT computing are demand dependent like broad network access, self-service, resource pooling, and speedy elastic nature. The common characteristics of cloud-IoT computing are homogeneity, massive scale, virtualization, resilient computing, low cost software availability, service orientation, geographic independent computation, and advanced safety availability. The cloud-IoT dependent internetworked distributive computation is internet based computation environment in which infrastructure, application software, and various similar / dissimilar platforms are accessible in the cloud and the end users (businessman, developers) have the right to use it as the client. Cloud is a step from Utility Computing and several industries / companies are frequently using cloud based systems in their day-to-day work. Therefore, safety issues and challenges of cloud computing cannot be avoided in the current era. Hence, the researchers must develop high order authentication protocols for preventing the safety threats of cloud based data communication systems..

The proposed CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) based management of cloud-IoT integrated information is a two phase authenticated encoding (AE) mechanism. The first phase is worn for executing privacy computations, and the second phase is used for computing validation and truthfulness. Here, both the cycles use same encoding technique. It is well known to us that the CCM/CCMP is an amalgamation of two forms namely AES counter form and CBC- MAC (cipher-block-chain message authentication code) protocol form. The counter form is worn to carry out encoding which guarantees data privacy whereas CBC-MAC is worn to attain data legitimacy and reliability. In this investigation work the author has investigated and critically analyzed the CCMP dependent safe Cloud-IoT integrated distributive mechanism for data / information management. The proposed approach further improves the overall security and performance of cloud-IoT integrated computing networks. Further, the author has solved the challenges of cloud-IoT computing by studying and analyzing major cloud-IoT computing safety concerns, and safety threats which are expected in future generation cloud computing systems. In this paper, the author has proposed CCMP & CBC-HMAC (Cipher-Block-Chain key Hash-Message-Authentication-Code) encoding protocol can be efficiently used for providing information safety and preventing various attacks when the data is being transferred between the Cloud and a local network. The prevention mechanism for unauthorized access of data within the cloud is also presented whose performance is highly satisfactory. A secure and flexible framework to support self-organize and self register of consumer's information in to the cloud network is designed and tested. The testing results of proposed analysis provides us very clear evidences that the PRF of CCMP is a superior and secure in contrast to that of CBC-HMAC.

Index Terms: Authenticated Encoding, Cipher Block Message Authentication, Cloud Management, Secure Cloud Networks.

1. Introduction

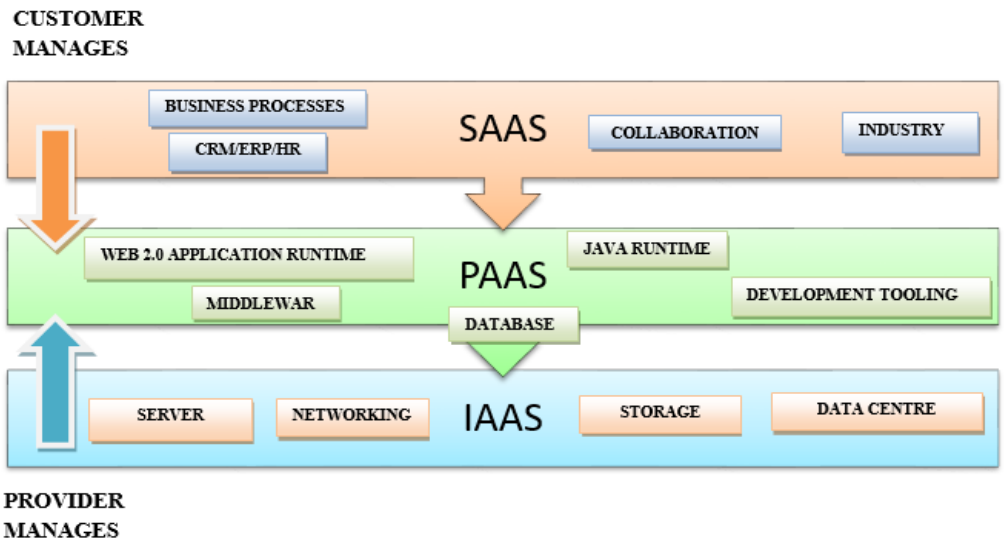
The cloud-IoT based computing is being frequently used in plentiful areas like business management, customer relationship supervision, communications and partnership, office efficiency suits, accounting applications, online storage management, electronic mails and shared calendars, human resource and employment etc. There are many benefits of cloud computing like scalability, 24/7 support, high order computing, pay as much as you use, virtual reality and dynamic communication systems. At the same time cloud computing has certain negative aspects like safety, lock-in, deficiency of power and trustworthiness. The safety is a major distress in cloud computing. So, in this research work the author is focusing on various protection concepts, issues, concerns, and safety threats [1, 2].

Copyright © 2020 MECS

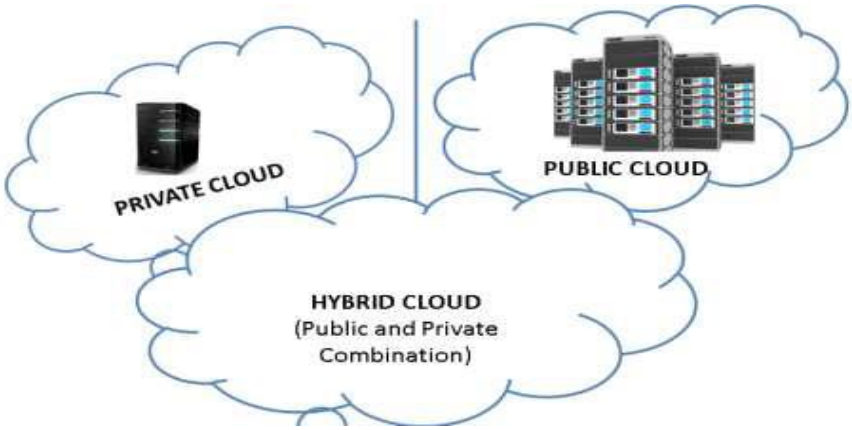
The NIST defined the Cloud Computing architecture by unfolding five important characteristics, three building blocks and four cloud deployment representations [3]. Further, NSIT defined three service representations of cloud computing which are known as Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). The SaaS provides the software and applications products to the users on demand throughout the internet. The PaaS provides the compatible platform to the users as per their demands across the global network for developing software products using available libraries and tools. The IaaS provides infrastructure to the users as per their demands across the internet.

The cloud representation is divided into four type's namely Private cloud, Community cloud, Public cloud and Hybrid cloud. In the case of Private cloud, the cloud infrastructure is provisioned for exclusive use by a single organization which has multiple consumers and numerous business units. In Public cloud, the cloud infrastructure is available for open use by the general public. In Community cloud, the cloud infrastructure is exclusively provided for specific community of consumers. In Hybrid cloud, the cloud infrastructure is a union of two or more dissimilar cloud infrastructures [3, 4]. The deployment of SaaS, PaaS and IaaS in a cloud network is presented in fig. 1(a) and fig. 1(b) where secure and speedy data access through IaaS, PaaS and SaaS will remain the main concern of end users and cloud facility providers in hybrid, protected and private clouds based distributive computing environment. The fig. 1(a) describes different ways of providing and managing customers' oriented services using of SaaS, PaaS and IaaS in a cloud computing network. The fig. 1(b) presents the cloud deployment model where private, protected and hybrid clouds will interact with each other for providing SaaS, PaaS and IaaS types of services to the customers in a secure cloud network. The cloud security supervision and providing efficient access of cloud services are the core concerns of this paper.

The current computing paradigms like single computing, distributed computing, software oriented architecture and networking are building blocks of cloud computing. There are many problems which are related to cloud computing paradigm. These problems can be divided into different categories namely Safety, Protection, Identity management, Resource management, Power / Energy management, Data isolation, Resource Availability, and Resource Heterogeneity [5, 6, 7]. There are several technologies and many leading companies which are providing cloud network services like Microsoft Cloud Technologies, Oracle Cloud Technologies, Oracle Mobile Clouds and Google Cloud Technologies. The Microsoft was the first to provide cloud technologies and applications which were sufficient for all types of business needs. The Microsoft provides all the three services i.e. SaaS, PaaS, and IaaS. For Infrastructure as a service, Microsoft provides Windows server and system canter. For Platform as a Service, it provides Windows Azure with which any one can build, host and scale applications in Windows data center. It also provides SQL SERVER and VISUAL STUDIO. For software as a Service, Microsoft provides office 365, office share point server, and dynamic CRM with exchange server facility [8, 9, 10].



1(a) Providing services using of SaaS, PaaS and IaaS in a cloud network.



1(b) The cloud deployment model.

Fig.1. The deployment of SaaS, PaaS and IaaS in a cloud Network [12, 13, 14].

The oracle also provides all types of cloud computing services (SaaS, PaaS and IaaS) to its customers. The oracle provides database as DaaS (Database as a Service) which consists of accessing and using the oracle database through network connection with complete development & operational environment. Anyone having a valid email ID can login with his / her credentials and can fully enjoy the trial version of Oracle database for a month. On later the person can decide his plans as per the needs [11, 12, 13, 14].

The oracle mobile cloud is a simple enterprise mobile connectivity which provides services like easy named interface, mobile APIs and other mobile applications for its enterprise systems. The mobile cloud provides additional amenities such as mobile Apps, Notifications (email, SMS, voice) and data synchronization to its customers. The Google cloud provides services such as Saas, PaaS and IaaS to its customers. The Google cloud also permits its developers and users to build, test and deploy their own applications on Google's highly scalable & fully protected infrastructure. The Google cloud provides infrastructure which allows Google to return billions of search results in a fraction of second. It also provides storage space of about 460 million Gmail users and serves billions of YouTube videos every month to the world. The Google cloud has ability to operate, build, and organize a gigantic network of servers and communication systems [15, 16, 17, 18].

In this research work the author has tried to solve the security challenges of cloud computing by studying and analyzing major cloud computing safety concerns, and safety threats which are expected in future generation cloud computing systems. Here, the author has proposed an encoding protocol known as the cloud CCMP (Counter Mode Cipher Block Chaining MAC Protocol) for information safety to prevent various attacks when the data is being transferred between the Cloud and a local network. The prevention mechanism for unauthorized access of data within the Cloud is also presented. A secure and flexible framework to support self-organize and self register of consumer's information in to the cloud network is designed. Further, in this research paper safe-cloud-IoT architecture for smart transportation / transmission system is designed and computationally analysis of proposed architecture is also presented.

The major research objective of this research work is to introduce CCMP based genuine encoding and decoding techniques which will be used for security enhancement of cloud-IoT integrated distributed computing systems. Further, compare the performance of proposed CCMP based genuine encoding & decoding techniques with existing CBC-HMAC technique in terms of *pass zone* and *fail zones* p_{values} using standard statistical data analysis tools in cloud computing environment. In the existing scenario, the CBC-HMAC based techniques are being mainly used for providing security in cloud-IoT integrated computing environment. But, it is observed by the author during experimental analysis of results that the CCMP based encoding and decoding techniques can provide better security than CBC-HMAC technique to the customers in the cloud-IoT integrated distributive computing environment. The author hopes that the use of CCMP based encoding and decoding techniques can provide further enhanced security to the customers while accessing IaaS, PaaS, and SaaS services in the cloud-IoT integrated distributive computing environment.

The body structure of this research work includes five sections namely introduction *(section I)*, literature review and theoretical foundation *(section II)*, the methodology *(section III)*, performance evaluation and statistical data analysis *(section IV)* and conclusions *(section V)*. The *section I* describes the need and interaction of cloud security related components. The *section II* describes about the theoretical foundations of cloud security concerns and review of existing literature. The *section III* describes the methodology for secure cloud computing framework and the CCMP based genuine encoding & decoding techniques. The *section IV* describes the performance evaluation and statistical data analysis of proposed methodology using average of mean and standard deviations of p_{values} *and* $1 - p_{values}$ for CCMP and CBC-HMAC techniques. The *section V* describes the concluding remarks and future research directions.

Copyright © 2020 MECS

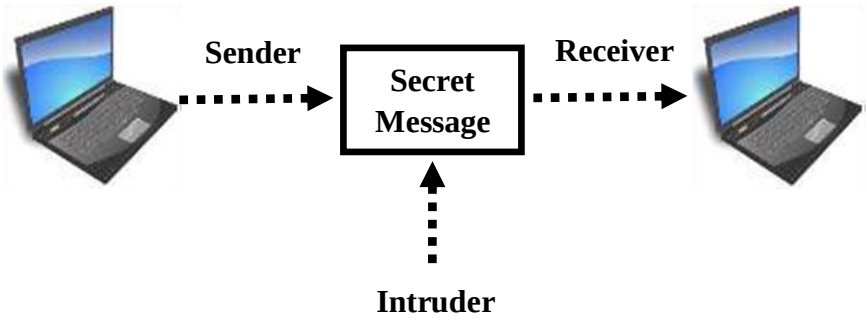
2. Literature Review and Theoretical Foundation of Cloud Security Concerns

Many of the researchers, academicians and industry experts have tried to describe the term cloud computing and its distinctiveness. The researchers Buyya et al. [10] have described as "Cloud is an analogous and dispersed computing system which consists of a group of interrelated virtualized computers and these computers are enthusiastically provisioned and accessible as one or more integrated computing assets recognized throughout cooperation between the service provider and customers."

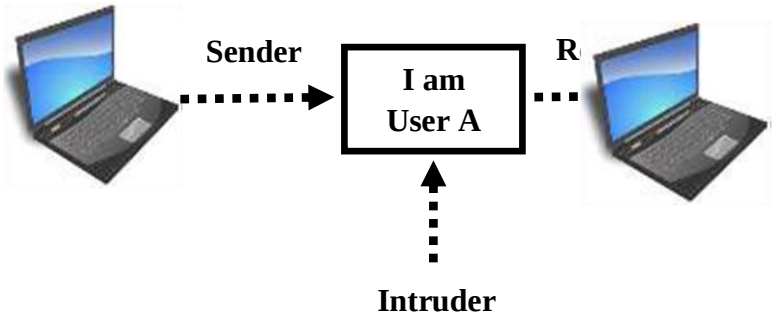
The authors Van Bon et al. [7] confirmed that a cloud is a huge collection of readily serviceable and reachable virtualized resources that may be enthusiastically reconfigured to fine-tune with a modifiable load and it optimizes the consumption of resources including IaaS, PaaS, and SaaS. The collections of resources in cloud-IoT integrated distributive computing environment are provided as per the rules of use-per-pay method. At this point of time the prevention of uncertainties are presented by the infrastructure provider according to rules and regulations described in the contract agreement. The researchers Miller [8] authentically said that the clouds are hardware dependent facilities that may provide distributive computations, internetwork and data / information storage abilities with astonishingly stretchable communication capabilities.

A report generated from Californian University, Berkeley [9] reveals that key properties of cloud-IoT based computing are inestimable computing wherewithal, use-per-pay and up-front commitment removal. Correspondingly, the researcher Alger D. [11] affirmed that the cloud-IoT integration is frequently used as the IT (information technology) infrastructure installed on an IaaS data center. The cloud-IoT integration based distributive computing is currently being used in many industries exhaustively. The cloud-IoT integrated computing has so many applications in different fields like customer relationship management, accounting applications, electronic mails, communications & collaboration, shared calendars, monetary management and office productivity suits etc. The cloud-IoT distributive computing has a blend of advantages like 24x7 support, pay-per-use, elevated computing, scalability, and virtualized dynamic environment [12].

The principles of safety are Confidentiality, Authentication, Integrity, Non repudiation, Availability and Access control. In Confidentiality only the sender and the receiver can share the information. By Interception Attack, confidentiality can be broken by listening to the communication between the sender and the receiver. The fig. 2(a) shows the loss of confidentiality due to interception attack e.g. packet sniffing or snooping [19, 20]. The lack of confidentiality in fig. 2(a) is due to the involvement of intruders while several data are being sent and received between sender and receiver.



2(a) Loss of confidentiality due to interception attack.



2(b) Loss of authentication due to fabrication attack

Fig.2. Loss of Confidentiality and Authentication Due to Interception and Fabrication Attacks.

The authentication identifies who is who in the communication network. The absence of authentication will increase fabrication attacks and masquerading. The fig. 2(b) shows the loss of authentication due to fabrication attack. The integrity ensures that the message from sender to receiver travels without alterations. The loss of message integrity is a type of modification attack e.g. some sites are *SSL 128 bit encoded*. In Non-Repudiation, the sender or the receiver cannot deny or refuse that the sender has not sent or the receiver has not received any message. The availability means that the resources /application must be available to authentic users as per service agreement. Attackers may disrupt the availability such as Denial of Service (DOS) [21, 22, 23, 24].

In order to manage the access control, a control access list is prepared which can provide us control and access related information like what can be accessed by whom. The two types of attacks are *active attack* and *passive attack*. In the case of active attack, the modification is done in the content of original message such as Masquerade, Modification, DOS and Replay. But, in the case of passive attack, there is no modification involved in the content of original message e.g. release of message contents & traffic Analysis. Some of the other attacks are packet sniffing or snooping, packet spoofing, phishing and socially engineered attacks. Since, the cloud-IoT integrated distributive computing is used by multi-users, numerous enterprises and varied infrastructure. Therefore, innovative cloud-IoT integrated distributed security concerns like velocity of attack, Multi-tenancy, data / information privacy, data / information assurance, and possession holding must be included in the design of next generation cloud computing systems.

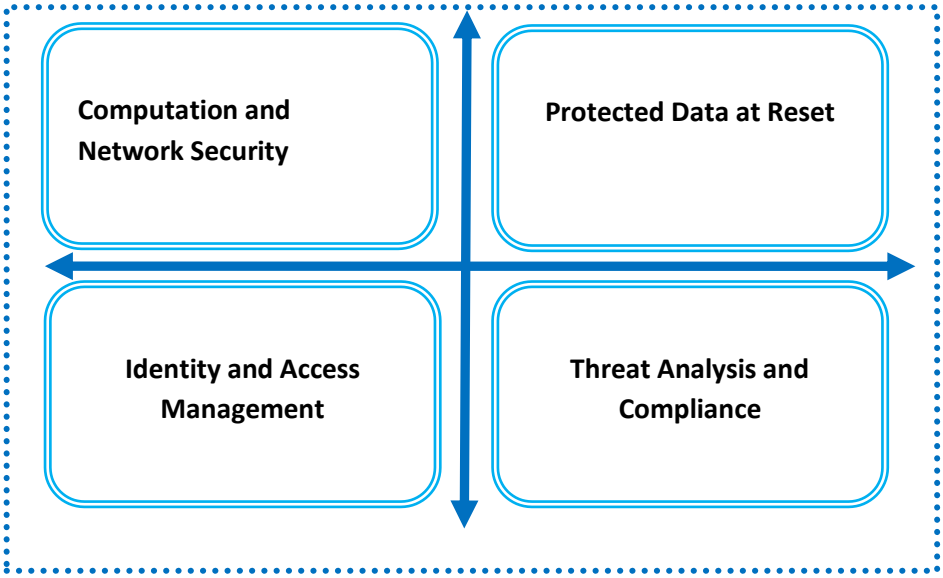


Fig.3. The Cloud-IoT integrated safety method

In order to make secure cloud-IoT integrated infrastructure, the researchers have used various cloud-IoT safety mechanisms. In a virtual cloud-IoT computing environment, the networks, storage, and computers are virtualized for maintaining safe keeping & security. The fig. 3 shows the Cloud-IoT integrated safety mechanisms [25, 26, 27].

2.1. Securing Physical Layer

It is to be guaranteed that the physical server can be protected in such a way that only certified users have authority to use the server. In order to secure physical layer safety, the network service provides access privilege to administrators, users and other work groups. The security providers can disable the unused hardware such as the NIC's, USB ports or drives in order to avoid copying of some malicious data by malicious users.

2.2. Securing Hypervisor

Hypervisor safety ensures that the hypervisor is not attacked by any attacker. Hypervisor is secured by installing safety updates and the software updates make sure that the software is up to date. The Hypervisor management system (HMS) can be accessed by configuring strong safety on the firewall between the management system and the network. The HMS provides direct access to administrators managing server. The administrators can prevent unauthorized access of cloud data by unknown users.

2.3. Securing Virtual Machines

The VMs (virtual machines) can be protected by hardening the virtual machines. The thing which may be the major point of attack in cloud-IoT integrated distributive system is the hardware meets software (HMS) network. The HMS will be able to control and manage the hypervisor. The security of VMs may further consist of virtual machine isolation (VMI) and VM hardening concepts. If one of the virtual machines of cloud-IoT integrated distributive network

Copyright © 2020 MECS

is suddenly attacked by network intruders and if it is by chance compromised then that specific virtual machine should be isolated from the remaining VMs for ensuring that the attackers don't get full command over the remaining virtual machines of the network and the corresponding infrastructure. The hardening is a way of changing the default configuration in order to achieve greater safety features. The denial of services (DoS) attacks can be prevented by restricting the resources which are to be consumed by virtual machines. The specific cloud-IoT integrated distributive operations like performing penetration testing of the guest operating systems and vulnerability scanning will be able to safeguard the virtual machines which are being used in cloud based systems [28, 29, 30, 31].

The operating system should be updated on very regular basis and the security related software products should be updated from time to time in the cloud-IoT integrated environment for managing the security related issues. The identity management is another concern because public cloud infrastructure has multiple users who are belonging to multiple organizations. The inclusion of multi-layers of safety like biometric authentication and multifactor authentication can make sure that only authentic users can login to the cloud-IoT integrated distributive computing system [2, 11].

In the case of federated identity management (FIM) multiple organizations use the data in a trusted and secure way by ensuring the authenticity of users e.g. it has been seen by the LinkedIn users that the LinkedIn Login is connected with Facebook Login page. The Facebook and LinkedIn might have establish a trust relationship with each other so that they are not aware of passwords but if you login to LinkedIn through facebook then facebook will tell LinkedIn in a software mechanism that this is an authorized user. The open ID is one of the standards for identity federation [32, 33, 34, 35].

2.4. One Time Passwords

Every new access request requires new password. It is a measure against *"password compromises"*. It enables organizations to authenticate their users of cloud service using the chosen identity provider. The users identities across different organizations can be managed together to enable collaboration on cloud. It is an open standard for decentralized authentication and access control and it can be used by allowing users to log onto many devices using the same digital identity.

2.5. Governing and Operating in Cloud-IoT integrated Computing Environment

The governance refers to the policies, processes, laws and institutions that define the structure by which companies are directed and managed. Every organization has its own safety policies and the competent authorities ensure that these well defined safety policies must be implemented at information technology level in the cloud-IoT integrated computing environment. Certain organizations like banking sector has its own set of rules & laws to ensure that the highly confidential data of the users like internet based account access and transactions related passwords and OTPs (One Times Passwords) must not be compromised at any cost. In the similar way, the mobile healthcare organizations have their own set of medical treatments related governing rules & laws. But, the m-health and other organizations must have to ensure that all the governing rules of that country's government should be followed by them or else the organization / company may be prosecuted because of violating rules.

In the cases of traditional data centers, the information technology (IT) department of that organization will have to take care of corresponding governing rules and regulations. But, in the case of cloud-IoT integrated computing atmosphere, the cloud service provider and the organization's IT department has the responsibility to make sure that the policies of organization & corresponding country are implemented in cloud-IoT integrated computing paradigm [36].

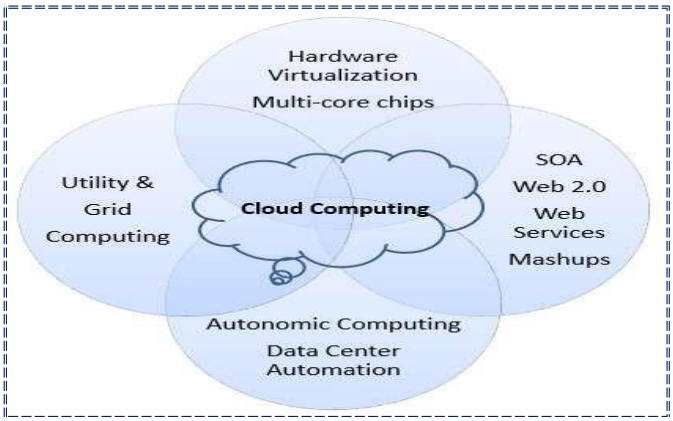


Fig.4. The overview of Governance and Operations in Cloud Networks.

Now, in the current era of cloud computing services can challenge several compliance audit necessities like data location and cloud computing safety policy transparency in agreement auditing efforts. The examples of the agreement

requirements include privacy and laws; Payment Card Industry (PCI) requirements; and monetary reporting laws [36, 37]. It may be possible that the data cannot be traced for a specific period of time in the cloud. But, on later the operating system of cloud server will know the exact location of data. Therefore, its fast retrieval will become possible in the situations of disaster. In the cloud computing representations, the primary cloud service provider may outsource capabilities to third parties who may also have outsourced the recovery process. This will further bring difficulty for the whole cloud computing system if the primary cloud service provider does not ultimately hold the cloud data. The fig. 4 shows an overview of cloud safety mechanism of cloud computing systems [20, 21, 38].

The intrusion detection software products play an important role in providing securities in cloud networks. These products are used at server level as well at the network level. At network level they do packet sniffing and see whether there is a pattern of attack in the network traffic and at server level they monitor the different operations that how the **process**es are accessing the system. They monitor the usage of operating system at server level and check there is an intrusion happened in our server and also prevents the attack. Data in cloud should only be accessed by authorize user. Data in cloud should not be accessed by an normal employee i.e. finance data cannot be accessed by the human resource (HR) department and HR department data cannot be accessed by any normal employee. So, role based access control (RBAC) is us in this situation. The BRAC provides additional level of safety and it ensures that only authorize can access the particular resource whether it is a website or a hardware of cloud computing systems [39, 40, 41, 42].

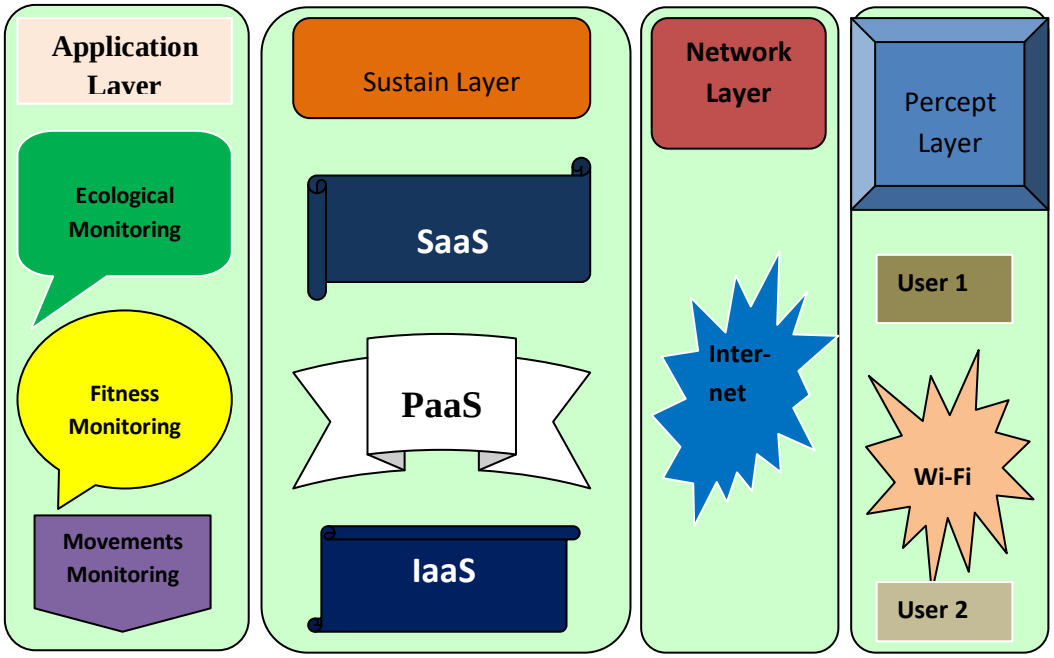


Fig.5. The SecC Framework for Cloud Networks [22, 24, 43, 44].

3. The Methodology

3.1. The Secure Cloud (SecC) Computing Framework

In the case of cloud services where user to server networking is needed, the encoding input 'K' lasts for the complete data transmission duration. In each session of cloud, a new encoding input needs a unique 13 bytes nonce value *N* for each encoded MAC Protocol Data Unit (MPDU). The nonce '*N'* confirms that duration of encoding inputs K are larger and any repeated attack will be traced and let down by the system. Here, '*N'* is built using 48 bits package numeral (PN), 48 bits target internet protocol address (A2), and 8 bits precedence [26]. Governance refers to the policies, processes, laws and institutions that define the structure by which companies are directed and managed [24, 43, 44, 45, 46].

The architectural views are the representation of overall design of the system. Web of Metadata (Capabilities, Categories, Configuration and Dependencies) is sensitive, personal and it includes corporate information which can be stored in both public and private clouds. It is an expanded view of metadata for creating new value streams and it mitigates information risk. In this way, cloud architectures allow greater degrees of sharing & collaboration and present new opportunities for information technology professionals. The testing, monitoring, diagnostics and verification tasks are required at different levels of cloud computing. The fig. 5 shows SecC framework of cloud computing system [45, 46, 47]. Generally cloud networks uses two-phase authentic encoding (AE) form for achieving a validation in first round (client round) and encoding in the next round (server round). The fig. 5 shows an example of a secure framework for smart services in which three layer architecture is offered [48, 49, 50].

Copyright © 2020 MECS

3.2. The CCMP Based Genuine Encoding Technique

The CCM/CCMP is a true encoding procedure which is also known as CCM creator dispensation. The procedure starts by using variation of CBC-MAC to work out the MIC label from the simple text MPDU, AAD and *nonce*. The MIC label is then updated to the MPDU and then these two are consequently encoded with the help of counter form. The CCMP does not need an independent method for decoding. The decoding is automatically concluded if once the MIC label is confirmed without any fault by the party pursuing decoding. In the case of CCM, a client can choose a MIC label value from a chain of 't' € {4,6,8,10,12,14, 16, 18, 20, 22} bytes. The CCMP yet has unchanged MIC label 't' = 8 [41].

In order to execute genuine encoding, CCM/CCMP uses five inputs i.e. encoding input '*K'*, nonce '*N'*, simple text *'M'*, Additional Authenticated Data AAD and a numeric significance for nonce ' ' . The encoding input K is 128 bits. This input is obtained during the IEEE four-way handclasp. The *nonce* 'N' is constructed from the 48 bits package numeral (PN), the 48 bits target IP address (A2), 8 bits precedence of MPDU header and its dimension is 13 bytes. The simple text M is the MPDU which excludes the 8 bytes MIC label and the 8 bytes MPDU header. The AAD is the additional authenticated data which is obtained from the MPDU header. Its size is 22 bytes to 30 bytes. The AAD is made up of frame control, source IP address, Destination IP address, source MAC address and quality control. The user will have to assign a value for the changeable nonce 'N' before implementing encoding method. The authenticated encoding **process** is described and presented in fig. 6.

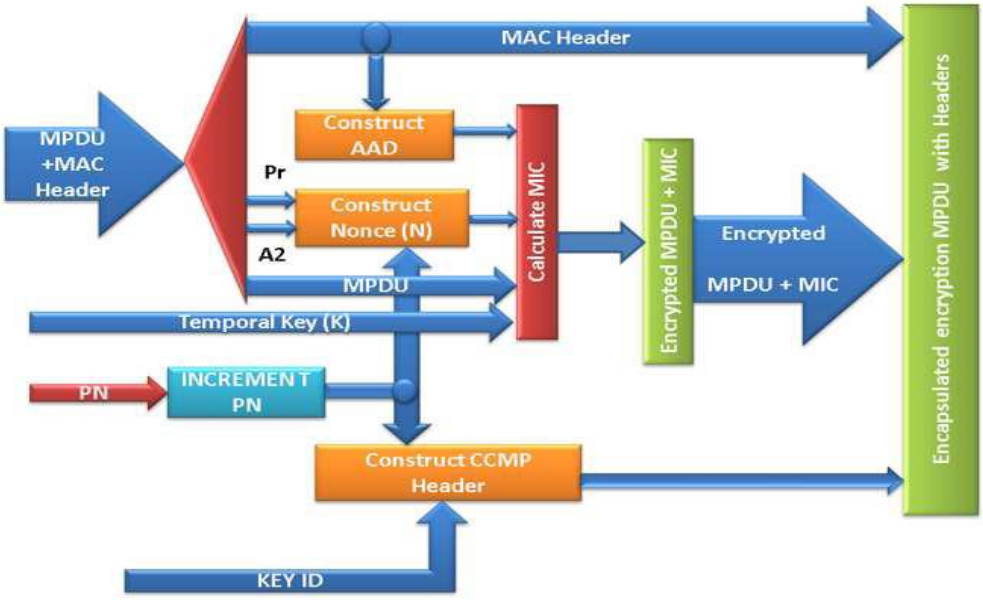
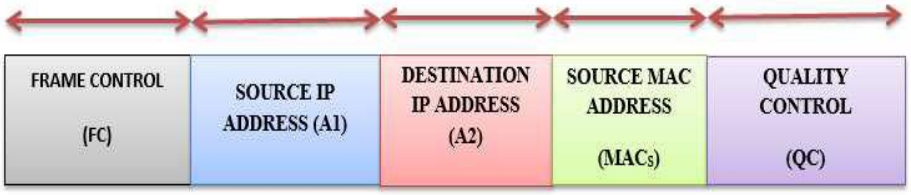
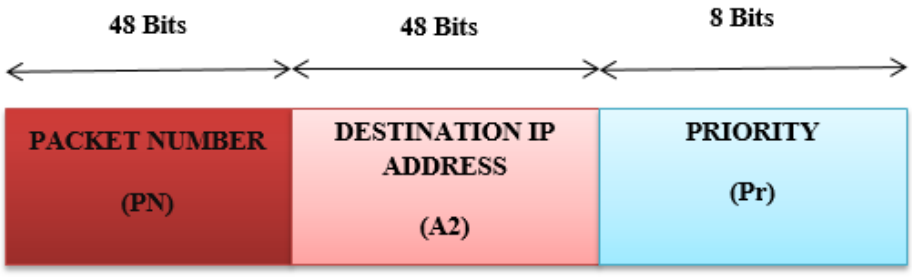


Fig.6. The CCMP based authenticated encoding [26, 54, 55].



7(a) The construction of Additional Authenticated Data (AAD)



7(b) The construction of Nonce (*N)*

Fig.7. The Additional Data Authentication and Nonce Construction in Authentication Encoding of Cloud Networks.

The value of package numeral (PN) is augmented every time using a counter for allocating an unmarked package numeral to each MPDU. Here, no redundancy of package numeral will occur for the identical encoded input. A novel AAD is created for all transmitted MPDU. The 13 bytes nonce *'N'* is created from 48 bits package numeral, 48 bits target IP address A2 and 8 bits precedence field of MPDU header. A fresh package numeral and key ID are used for designing CCMP header.

The encoding input K, AAD, nonce *'N'* and simple text data M will now be used to calculate the value of cipher-text 'C' and MIC label ('t'). The cipher text and MIC label are computed using existing algorithms and their encapsulation outcomes are transmitted as authentic encoded data to the recipient. The fig. 6 shows the diagrammatical description and implementation of reliable encoding technique which generates the Cipher text ('C') and MIC label ('t') [51, 52]. The construction of 13 bytes nonce *'N'* from PN, target IP address A2 and the precedence field of MPDU header is presented in figures 7(a) and 7(b) which will represent the Additional Authentication Data (AAD) and *nonce* (*N*) [53, 54].

3.3. The CCMP Based Genuine Decoding Technique

The CCMP authenticated decoding method uses following five inputs:

Input 1: The 128 bits encoding input '*K'* which is obtained from IEEE 4-Way Handshake.
Input 2: The 13 bytes Nonce *N.*
Input 3: The encapsulated MPDU. This excludes the MIC label and MPDU header). *Input 4:* The AAD which is 22bytes to 30 bytes and it was obtained previously.
Input 5: The changeable nonce *'N'* which has already been derived in the encoding method.

After putting these five inputs at right position the legitimate decoding method will be initiated using following steps [26]:

Step 1: The encapsulated MPDU is uncovered of MAC header and CCMP header.
Step 2: The new AAD is created from the uncovered MAC header.
Step 3: The nonce 'N' is created from PN, A2 and precedence.
Step 4: The MIC label *'t'* is obtained from the encoded MPDU after processing.
Step 5: The encoding input K, Nonce N, and encoded MPDU are calculated for creating the original simple text MPDU. This calculation is completed by encoding the encoded MPDU.
Step 6: The Nonce N, new AAD and encoding input K, are calculated for creating the new MIC label 't'.
Step 7: Now, the latest and aged MIC labels are compared for verifying the accuracy and reliability of the ADD and encoded MPDU.

The proposed method is assume to be thriving if 't=00' otherwise *FALL SHORT* communication message will be demonstrated. In this technique the CCMP doesn't need a separate decoding method because the decoding is involuntarily completed if once the authenticity of MIC label 't' is confirmed without any error. The decoding method of CCMP authenticity verification can be represented by fig. 8 [51, 52, 53].

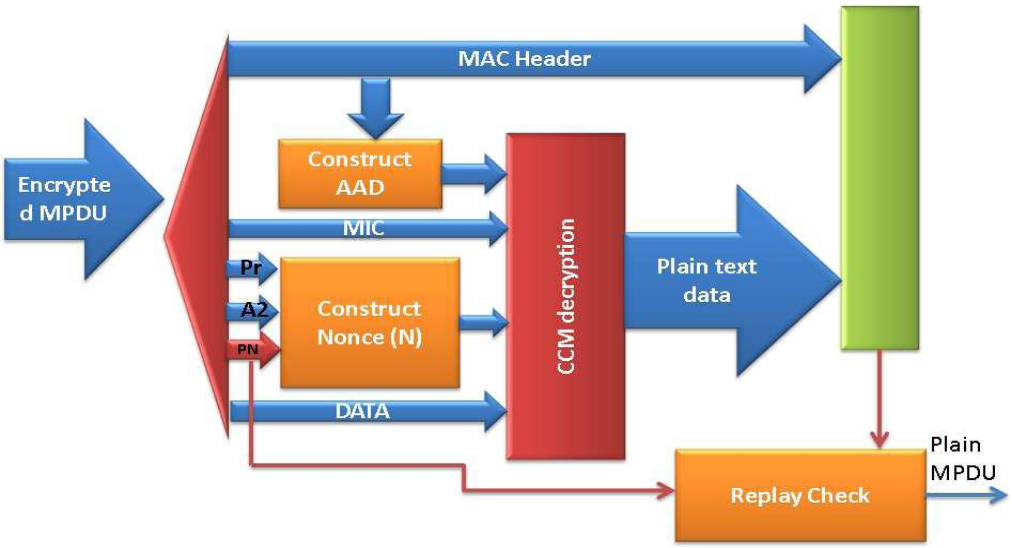


Fig.8. The CCMP Based Authenticated Decoding.

4. Performance and Statistical Analysis of Secure Cloud Networks

The unpredictability is a probabilistic characteristic. The certain existing methods can be used to explain and analyze the concept of probability. The researchers [42, 44, 46] used a geometric tool called DIEHARD [48] for verifying the pseudo-randomness personality of RSA's BSASE and JSAFE random number generation algorithms. The analysis of geometric results proves that JSAFE and BSAFE are accurate for originating pseudo-random series of numbers. The NIST of USA used geometric analysis tool which included 18 tests for selecting Rijndael block cipher in order to replace 3DES [40]. The Rijndael was selected by AES block cipher as a better option for pseudo-random number generation because of its best performance.

The exercise of geometric study in analyzing the performance of cryptographic systems can never be overlooked. The researcher Alani [36] used DIEHARD geometric tool for investigating the randomness distribution of zeros and ones for the cipher texts which were generated by AES-256, 3DES, Blowfish-448 and Serpent-256. Here, simple graphs were used to understand the geometric results which were based on 50 – 50 distribution of zeros and ones. Alani used p_{values} from every test to design graphs which were having three regions namely Doubt, Safe and Fall-short. The outcomes proved that Blowfish-448 and AES-256 have best distribution of p_{values} in safe region. Further, NIST [40] geometric test agreed with the results Alani [36] and proved that AES is a superior *Pseudo Randomness Function (PRF)*. The task of author in this geometric analysis is to examine and prove that CCMP is as good as CBC-HMAC (Cipher-Block-Chain key Hash-Message-Authentication-Code) or CCMP is better than CBC-HMAC.

If the data of simple text is encoded by a PRF then the cipher text generated will be a muddled up allocation of '0's and '1's in the result. This allotment of 0''s and '1's must be 50% - 50% for a superior PRF [30, 18]. Every geometric investigation test is a simulation and integration of different test stages. Any particular test has the capacity to include a wide range of simulation related problems and it can expose all the safety linked problems which were never taken into considerations in theoretical study of systems. The geometric testing of CCMP and CBC-HMAC encoding technique without viewing the corresponding source codes can help us in understanding and measuring the performance of these approaches without any discrimination. Further, it is the fact that the superiority of forecast in geometric investigation tests remains convincing on the majority of occasions. Therefore, a believable logical move is essential for analyzing the PRF behavior of CCMP and CBC-HMAC techniques.

4.1. The Selection of 48-bit IP Addresses for CCMP and CBC-HMAC

It is continuously observed by the researchers that the 32-bits IPV4 addressing scheme is little short for video communication in cloud and IoT based environment whereas 128-bits IPV6 addressing scheme occupies large amount of memory space and it has high memory wastage. Therefore, to overcome these problems of IPV4 and IPV6 the authors used 48-bits IP addresses in developing CCMP and CBC-HMAC communication protocols. The 48-bit IP addressing scheme is compatible with 32-bits IPV4 and 128-bits IPV6 address.

The 1st address, 2nd address, 2nd last address and last address of 48-bits addressing scheme can be written as follow:

1st address = {00000000; 00000000; 00000000; 00000000; 00000000; 00000000}

2nd address = {00000000; 00000000; 00000000; 00000000; 00000000; 00000001}

..

..

..

2nd last address = {11111111; 11111111; 11111111; 11111111; 11111111; 11111110}

Last address = {11111111; 11111111; 11111111; 11111111; 11111111; 11111110}

The total number of addresses generated in 48-bits IP addressing scheme of CCMP and CBC-HMAC communication systems will be 2^{48}(281 trillion addresses approximately) where each address will be of 48-bits. These many addresses are more than enough for storing video images and voice signals in cloud and internet of Things (IoT) based computing environments.

The total number of addresses generated in 32-bits IP addressing scheme of *IPV4* is 2^{32} (4.29 billion addresses approximately) where each address is of 32-bits. These many addresses are very short for storing video images and voices signals in cloud and IoT based computing environments. Therefore, high speed video communication using IPV4 is not possible in cloud and IoT based environment. If we map 32-bits IP addresses of IPV4 with 48-bits IP addressing scheme of CCMP / CBC-HMAC then this mapping can be represented by Eq.(1).

$$(IP\ Address\ Space\ of CCMP\ or\ CBC_{HMAC}) = (2^{16} \times (IP\ Address\ Space\ of\ IPV4) \quad (1)$$

The total number of addresses generated in 128-bits IP addressing scheme of *IPV6* is $2^{128}(3.40 \times 10^{26}\ trillions)$ addresses approximately where each address is of 128-bits. These are huge amount of addresses and are far beyond the

amount of addresses required for our day-to-day video communication in cloud and IoT based communication environment. Hence, video communication using IPV6 will have huge amount of wastage of memory space while providing video communication between end users in cloud and IoT based environment. If we map 128-bits IP addresses of IPV6 with 48-bits IP addressing scheme of CCMP / CBC-HMAC communication approach and 32-bits IP addressing scheme of IPV4 then this mapping can be represented by Eq.(2) and Eq.(3).

$$IP\ Address\ Space\ of\ IPV6 = 2^{80} \times (IP\ Address\ Space\ of\ CCMP\ or\ CBC_{HMCA}) \quad (2)$$

$$\text{IP Address Space of IPV6} = 2^{96} \times (\text{IP Address Space of IPV4}) \quad (3)$$

The computational analysis of Eq.(1), Eq.(2), and Eq.(3) shows that the amount of address space occupied by 48-bits IP addressing scheme of CCMP / CBC-HMAC is in the multiples of IPV4 and IPV6. Further, the CCMP and CBC-HMAC approaches are compatible with IPV4 and IPV6 addressing schemes. Hence, integration of CCMP and CBC-HMAC approaches with IPV4 or IPV6 communication environment will be easily possible.

4.2. The Selection of Statistical Testing Tool

Choosing a geometric test toning set above the other involves considerations of several factors e.g. effortlessness of use, minimizing the needs of computing, and exactness. In current era NIST test suite is being frequently used by researchers and scientists for geometric analysis and testing.

In order to generate convincing geometric test results, this investigation requires using the sample data of size ≥ 1024KB. After conducting rigorous robustness testing the author found that the DIEHARD test suite effectively processed 18MB sample data file which was separately encoded using CCMP and CBC-HMAC. On the other side it was seen by author that The NIST test suite crashed several times while processing the sample data of size ≥ 1024KB. This experiment reveals that DIEHARD geometric testing tool gives better performance than NIST [48]. Hence, the author used DIEHARD tool for geometric testing. The table 1 presents 18 DIEHARD geometric tests and corresponding relevant p_{values} [34, 40].

4.3. The Selection of Experimental Data

The 20MB *colororacle.org* file was used as sample for this experiment. This file was independently encoded using CCMP and CBC-HMAC encoding techniques. The ensuing cipher texts, *colororacle.ccmp* and *colororacle.cbc-hmac* were forwarded into the eighteen DIEHARD geometric tests to yield *colororaclereport.ccmp* and *colororaclereport.cbc-hmac*. These reports generated approximately 242 p_{values}. The p_{values} generated in the *colororaclereport.ccmp* and *colororaclereport.cbc-hmac* were the quantification of random distribution for '0's and '1's in *colororacle.log* after encoding it by CCMP and CBC-HMAC.

Table 1. The Statistical Tests for DIEHARD and the corresponding p_{values}

Type of DIEHARD Test Conducted		p_{values}	***Chi Square Test***	***KS-TEST***
1.	Binary Position Test of 32x32 Matrices	2	√	√
2.	Birthday Spacing Test	9	×	√
3.	Bit Flow Test	20	×	×
4.	Overlapping Five Combination Test	10	×	√
5.	The OQSO	29	×	×
6.	Binary Position Test 8x10 Matrices	25	×	×
7.	Count the '1's Test on Flow of byte	2	√	×
8.	Binary Position Test 34x34 Matrices	3	√	×
9.	The Smallest Distance Test	20	√	√
10.	Count the '1's Test for particular byte	26	√	×
11.	The Craps Test	2	√	√
12.	The 3D Sphere Test	20	×	√
13.	The Overlapping Sums Test	3	×	×
14.	The OPSO	24	×	×
15.	The Runs Test	4	×	×
16.	The DNA Test	31	×	×
17.	The Parking Bundle Test	10	×	√
18.	The Compress Test	2	√	×
Sum of Results		242	7	7

4.4. Defining Importance Level (α)

The variable α is defined as the chance of discarding a *Null Assumption* even if it is accurate. It is also known as *category I defect.* If a researcher considers the testing of PRF in safety form then he / she should present α as the chance that the test will give negative results despite the fact that the form is a true PRF. In other words α is the smallest prearranged value under which a *Null Assumption can* be discarded. Here, $0.01 \le \alpha \le 0.31$. For the purpose geometric test α is watchfully fixed near to 0.05.

4.5. The Assessment of p_{values} and $1 - p_{values}$

The p_{value} is also called as *probability* / *possibility value.* The p_{value} represents the possibility for a specified statistical representation that if the *Null Assumption* is exact then the statistical review will be alike or superior to the actual experimental outcome. However, Johnson's explanation of p_{value} has been disproved by researchers [42, 43]. The author argued that there is nothing random about whether a *Null Assumption* is true or false. This research work defines p_{value} as the determination of supremacy of evidence observed in experimental data besides H_0. The p_{value} is interrelated to α and H_0. The H_0 is acknowledged if $p_{value} \geq \alpha$, and is abandoned if $p_{value} < \alpha$ [2].

4.6. The Estimation of Guarantee Point

The researchers [42, 43, 44] recommended that guarantee point provides more information than p_{values}. The researcher [43] raised a question that "A confidence interval provides both an estimate of the effect size and a measure of its uncertainty". For the purpose of geometric test the guarantee point is calculated using following procedure:

$$(1-\alpha)\times 100\% = (1-0.050)\times 100\% = 95.00\%$$

4.7. The Estimation of Null and Alternate Assumptions

Definition 1: *Null Assumption* (*H_0)* was defined by [41] which is the declaration about the geometric allocation of one or additional variables in a specified trial data. In the proposed analysis H_0 is used to compare the PRF of CCMP and CBC-HMAC.

Definition 2: The *Alternate Assumption (H_i)* was defined by [41]. It is the substitute declaration for the geometric distribution of variables in a specified trial data. The value of H_i is believed to be true if *Null Assumption* fails. The *Alternative Assumption* (H_i) is used in the geometric analysis of this research work to prove that CCMP is superior to CBC-HMAC.

4.8. The Estimation of Success and Fall Short Criteria

After understanding the research of [36] and [42], this research has adapted the proposed approach as the root for defining the pass and fall short criteria. Therefore, the fall short and pass used by the proposed work for interpretation of results are accurate and trouble-free.

The next source for deciding pass and fall short criteria is connotation stage, which is set at 0.050 (5%). It gives confidence level of (1.0 - 0.050)×100% = 95.00%. Each set of 242 p_{values} are converted into a diagram. Here, every graph is divided horizontally and vertically into different key areas using following inference rules (IRs):

IR_1: The p_{values} less than the 0.050 significance point are in the *Fall Short Zone (F_{ZA}).* Therefore, these values will be considered as fall short test cases.

IR_2: The certain p_{values} which are equal to or below 0.00 levels are considered as *Completely Fall Short Zone (CF_Z).* These p_{values} will play a deciding role in the case of equal score conditions.

IR_3: The p_{values} greater than or equal to 0.050 and less than 0.40 are in the *Tolerable Zone (T_Z)* Therefore, these values are tolerable.

IR_4: The p_{values} greater than or equal 0.40 and less than 0.60 are considered within perfect region called *Ideal Zone (I_Z).* These p_{values} values are imminent for 50%-50% predictable distribution of '0's and '1's.

IR_5: The p_{values} greater than or equal to 0.60 and less than 0.95 are in *Satisfactory Zone (S_Z).* Therefore, these p_{values} are fine and adequate.

IR_6: The p_{values} equal to 0.95 are assumed to be *Good Enough Zone (GE_Z).*

IR_7: The p_{values} greater than 0.95 are assumed to have entered in *Fall Short Zone (F_{ZB})* beyond Assurance point.

It is very clear from these rules that an excellence quality PRF should have maximum p_{values} in the range of IR4 and minimum p_{values} in the range of *IR_1*, *IR_2* and *IR_7*. If two techniques have same PRF values in the range of *IR4* then different possible combinations of the union of *IR_3*, *IR_4*, *IR_5*, and *IR_6* should be used for making decisions.

After analyzing the above inference rules from IR_1 to IR_7 the author firmly states that the conditions represented by Eq.(4) to Eq.(11) will always remain true where as Eq.(12) and Eq.(13) may or may not be true if and only if CCMP is a better PRF than that of CBC-HMAC:

$$\{\mathrm{CCMP}[\mathrm{F_{ZA}}(\mathrm{p_{value}})] + \mathrm{CCMP}[\mathrm{F_{ZB}}(\mathrm{p_{value}})]\} \leq \{\mathrm{CBC\_HMAC}[\mathrm{F_{ZA}}(\mathrm{p_{value}})] + \mathrm{CBC\_HMAC}[\mathrm{F_{ZB}}(\mathrm{p_{value}})]\} \quad (4)$$

$$\{\mathrm{CCMP}[\mathrm{F_{ZA}}(\mathrm{p_{value}})] + \mathrm{CCMP}[\mathrm{CF_{Z}}(\mathrm{p_{value}})]\} \leq \{\mathrm{CBC\_HMAC}[\mathrm{F_{ZA}}(\mathrm{p_{value}})] + \mathrm{CBC\_HMAC}[\mathrm{CF_{Z}}(\mathrm{p_{value}})]\} \quad (5)$$

$$\{\mathrm{CCMP}[\mathrm{F_{ZA}}(\mathrm{p_{value}})] + \mathrm{CCMP}[\mathrm{CF_{Z}}(\mathrm{p_{value}})] + \mathrm{CCMP}[\mathrm{F_{ZB}}(\mathrm{p_{value}})]\} \leq \{\mathrm{CBC\_HMAC}[\mathrm{F_{ZA}}(\mathrm{p_{value}})] + \mathrm{CBC\_HMAC}[\mathrm{CF_{Z}}(\mathrm{p_{value}})] + \mathrm{CBC\_HMAC}[\mathrm{F_{ZB}}(\mathrm{p_{value}})]\} \quad (6)$$

$$\{\mathrm{CCMP}[\mathrm{T_{Z}}(\mathrm{p_{value}})] + \mathrm{CCMP}[\mathrm{I_{Z}}(\mathrm{p_{value}})] + \mathrm{CCMP}[\mathrm{S_{Z}}(\mathrm{p_{value}})]\} > \{\mathrm{CBC\_HMAC}[\mathrm{T_{Z}}(\mathrm{p_{value}})] + \mathrm{CBC\_HMAC}[\mathrm{I_{Z}}(\mathrm{p_{value}})] + \mathrm{CBC\_HMAC}[\mathrm{S_{Z}}(\mathrm{p_{value}})]\} \quad (7)$$

$$\{\mathrm{CCMP}[\mathrm{F_{ZA}}(1 - \mathrm{p_{value}})] + \mathrm{CCMP}[\mathrm{F_{ZB}}(1 - \mathrm{p_{value}})]\} \leq \{\mathrm{CBC_{HMAC[F_{ZA}(1-p_{value})]}} + \mathrm{CBC_{HMAC[F_{ZB}(1-p_{value})]}}\} \quad (8)$$

$$\{\mathrm{CCMP}[\mathrm{F_{ZA}}(1 - \mathrm{p_{value}})] + \mathrm{CCMP}[\mathrm{CF_{Z}}(1 - \mathrm{p_{value}})]\} \leq \{\mathrm{CBC\_HMAC}[\mathrm{F_{ZA}}(1 - \mathrm{p_{value}})] + \mathrm{CBC\_HMAC}[\mathrm{CF_{Z}}(1 - \mathrm{p_{value}})]\} \quad (9)$$

$$\{\mathrm{CCMP}[\mathrm{F_{ZA}}(1 - \mathrm{p_{value}})] + \mathrm{CCMP}[\mathrm{CF_{Z}}(1 - \mathrm{p_{value}})] + \mathrm{CCMP}[\mathrm{F_{ZB}}(1 - \mathrm{p_{value}})]\} \leq \{\mathrm{CBC_{HMAC[F_{ZA}(1-p_{value})]}} + \mathrm{CBC\_HMAC}[\mathrm{CF_{Z}}(1 - \mathrm{p_{value}})] + \mathrm{CBC\_HMAC}[\mathrm{F_{ZB}}(1 - \mathrm{p_{value}})]\} \quad (10)$$

$$\{\mathrm{CCMP}[\mathrm{T_{Z}}(1 - \mathrm{p_{value}})] + \mathrm{CCMP}[\mathrm{I_{Z}}(1 - \mathrm{p_{value}})] + \mathrm{CCMP}[\mathrm{S_{Z}}(1 - \mathrm{p_{value}})]\} > \{\mathrm{CBC\_HMAC}[\mathrm{T_{Z}}(1 - \mathrm{p_{value}})] + \mathrm{CBC\_HMAC}[\mathrm{I_{Z}}(1 - \mathrm{p_{value}})] + \mathrm{CBC\_HMAC}[\mathrm{S_{Z}}(1 - \mathrm{p_{value}})]\} \quad (11)$$

$$\{\mathrm{CCMP}[\mathrm{I_{Z}}(\mathrm{p_{value}})]\} \gtrsim \{\mathrm{CBC\_HMAC}[\mathrm{I_{Z}}(\mathrm{p_{value}})]\} \quad (12)$$

$$\{\mathrm{CCMP}[\mathrm{I_{Z}}(1 - \mathrm{p_{value}})]\} \gtrsim \{\mathrm{CBC\_HMAC}[\mathrm{I_{Z}}(1 - \mathrm{p_{value}})]\} \quad (13)$$

4.9. Experimental Analysis of Outcomes and Discussions

It is observed that the easiest and almost correct way to display the outcome is to utilize graphical symbols for representing all p_{values} which are originated from the geometric tests. The total of 242 p_{values} which were obtained from each test is used to propose the graphs presented in figures 9, 10, 11 and 12.

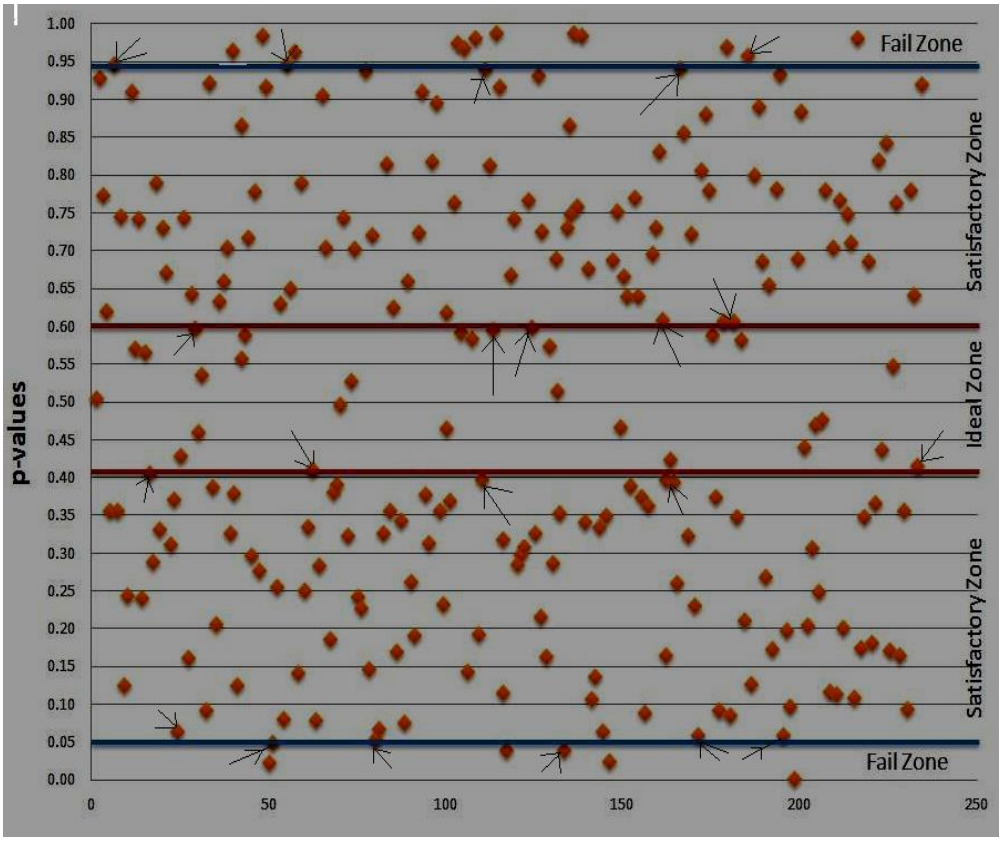


Fig. 9. Distribution of p_{values} for CCMP [26, 54, 55].

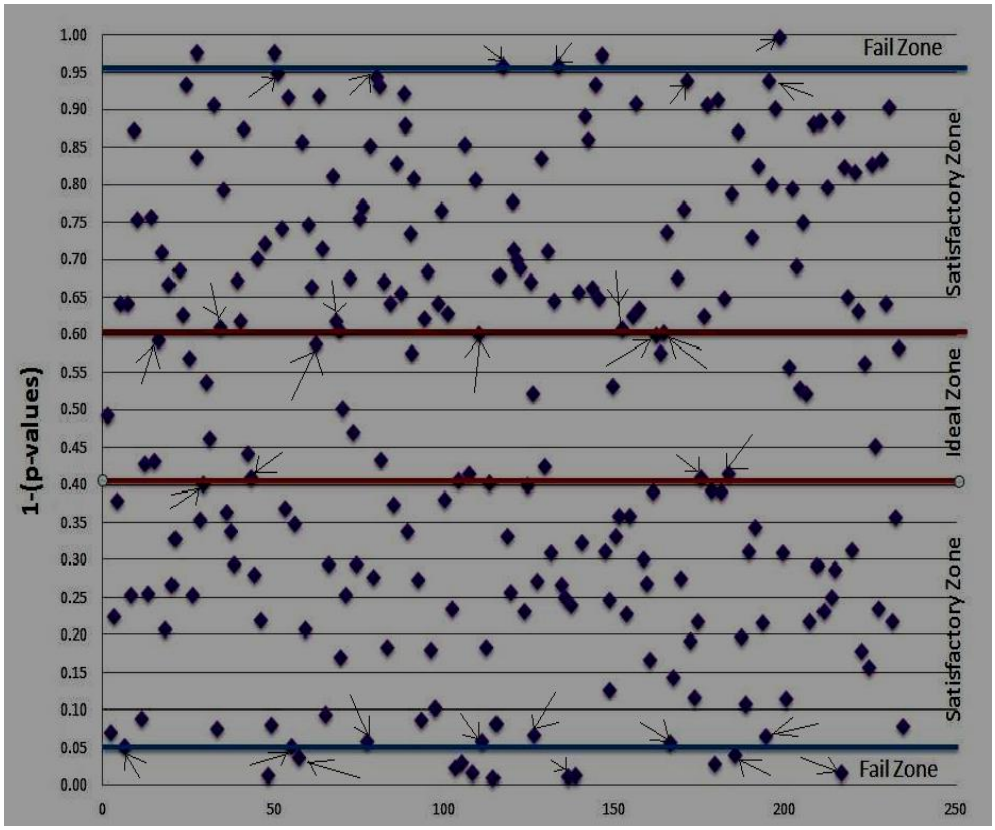


Fig.10. Distribution of $1 - p_{values}$ for CCMP [26, 54, 55].

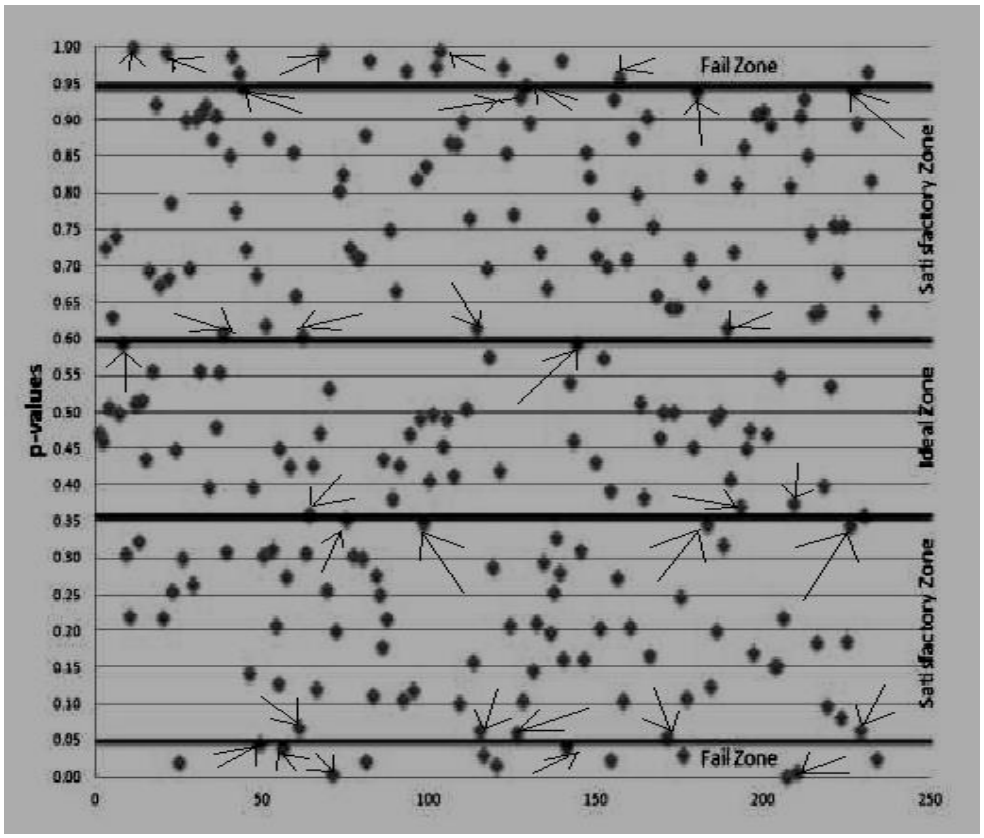


Fig.11. Distribution of p_{values} for CBC-HMAC system [26, 54, 55].

The number of p_{values} for CCMP and CBC-HMAC in F_{ZA}, CF_Z, T_Z, I_Z, S_Z, GE_Z, and F_{ZB} were counted for evaluating the performances. As per fig. 9 it was observed that the CCMP gave 10 p_{values} in F_{ZB} and approximately 4 p_{values} in F_{ZA}. Therefore, total number of p_{values} in F_{ZA} + F_{ZB} + C_{FZ} is approximately fourteen. In between it was observed that approximately 28 to 30 p_{values} in I_Z area and approximately 228 p_{values} in the range of T_Z, I_Z, S_Z, and GE_Z areas.

The records of [48] showed that there are two variants of the DIEHARD geometric tool. One variant is in "C" binary and the other variant is in Fortran Language. The literature implied that the two variants compute p_{values} in mirror image of each other. One variant computes p_{values} and the other computes $1 - p_{values}$. At this stage it is decided to compute and draw the equivalent $1 - p_{values}$ for each p_{values}. The diagrammatical representation of p_{values} and $1 - p_{values}$ have shown their symmetric behavior.

The fig. 10 presents the distribution of 242 of $1 - p_{values}$ for CCMP. The distribution of $1 - p_{values}$ in fig. 10 is the mirror representation of fig. 9. There are four $1 - p_{values}$ in the F_{ZB} area. There are approximately twelve $1 - p_{values}$ in the FZA area. The total number of $1 - p_{values}$ in the I_Z, and IR_3, IR_4, IR_5, IR_6 rules based zones still remained unaffected.

The fig. 11 presents the allocation of p_{values} for CBC-HMAC approach. With reference to fig. 11, CBCHMAC has shown 14 p_{values} in the F_{ZB} area and 14 p_{values} beneath the 0.05 significance level (F_{ZA} area). There are approximately 55 p_{values} in the ideal zone. In over all, CCMP recorded roughly 14 p_{values} in F_{ZA} + F_{ZB} + CF_Z zones whereas CBC-HMAC showed approximately twenty seven to twenty eight p_{values} in these zones. Here, golden rule is that the technique having lowest number of p_{values} in all types of *Fall Short Zones* will be considered as the best algorithm. Therefore, it can be confirmed from the p_{values} of F_{ZA}, F_{ZB}, and CF_Z for CCMP and CBC-HMAC protocols that the PRF of CCMP is better than that of CBC-HMAC.

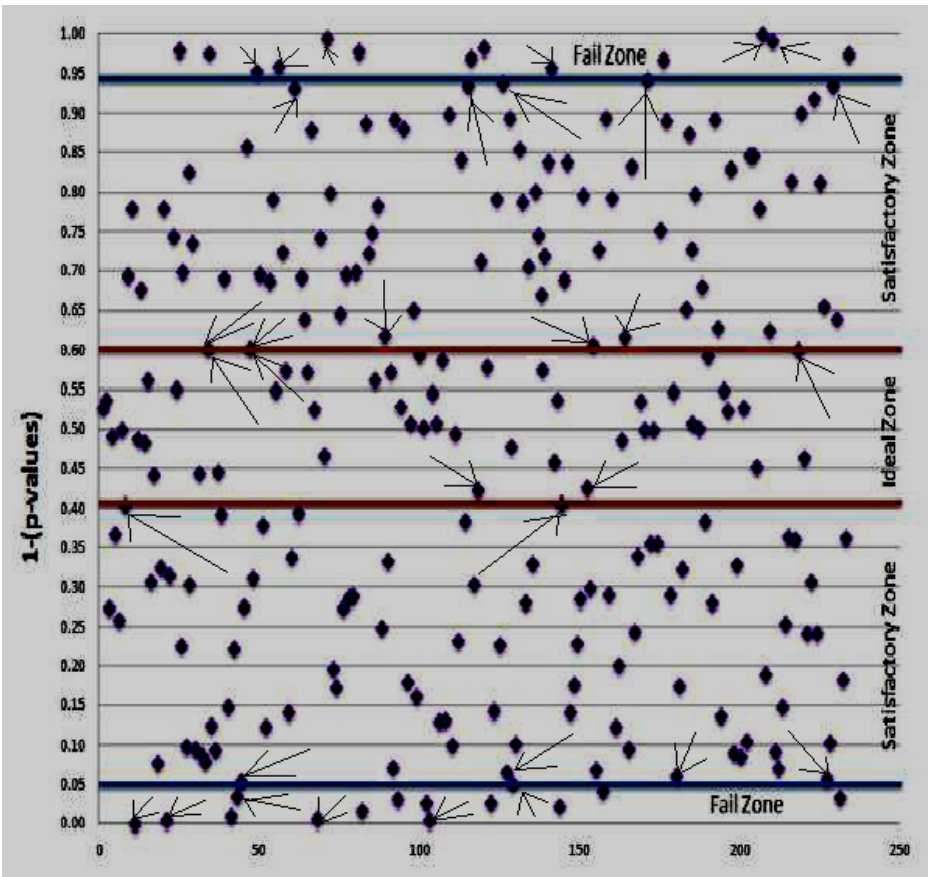


Fig.12. The distribution $1 - p_{values}$ for CBC-HMAC [26, 54, 55].

Table 2. The p_{values} and $1-p_{values}$based performance comparison of CCMP and CBC-HMAC [26, 54].

Zone Name	CCM / CCMP		CBC-HMAC	
	Approximate p_{values}	Approximate $1-p_{values}$	Approximate p_{values}	Approximate $1-p_{values}$
F_{ZA}	03	05	07	05
CF_Z	01	06	03	06
T_Z	100	95	67	80
I_Z	30	32	57	45
S_Z	86	86	75	47
GE_Z	12	10	07	08
F_{ZB}	10	08	11	10

The fig. 12 presents the distribution of 242 of $1-p_{values}$ for CBC-HMAC. The distribution of $1-p_{values}$ in fig. 12 is the mirror representation of fig. 10. There are approximately ten $1-p_{values}$ in the F_{ZB} zone. There are approximately twelve $1-p_{values}$ in the F_{ZA} fall short zone. The total number of $1-p_{values}$ in the T_Z, I_Z, S_Z, and GE_Z zones for fig. 12 still remained unaffected. The comparison of p_{values} and $1-p_{values}$ for CCMP and CBC-HMAC in different zones which are based on IR_1 to IR_7 can be represented by table 2.

It seems from table 2 that the performance of CBC-HMAC is better than that of CCMP if and only if ideal Zone (I_Z) p_{values} and the corresponding *1-(p_{values})* are taken into considerations because CCMP recorded thirty p_{values} in the ideal zone whereas CBC-HMAC recorded fifty seven p_{values} in ideal zone. Similarly, CCMP recorded thirty two $1-p_{values}$ in I_Z area whereas CBC-HMAC recoded forty five $1-p_{values}$ in the same area. But, the author suggests that considering only I_z values for concluding final result will be unfair and incomplete.

Therefore, the author has constructed matrices for all fall short zones and all pass zones collectively for comparing the overall performance of CCMP and CBC-HMAC. The matrices of all fall short zones (F_{ZA}, CF_Z, F_{ZB}) and all pass zones (T_Z, I_Z, S_Z, GE_Z) for CCMP and CBC-HMAC can be represented by Eq.(14), Eq.(15), Eq.(16) and Eq.(17):

$$CCMP_{fail_{zone}} = \begin{matrix} & CCMP_{p_{value}} & CCMP_{1-P_{value}} \\ F_{ZA} & 03 & 05 \\ CF_Z & 01 & 06 \\ F_{ZB} & 10 & 08 \end{matrix} \quad (14)$$

$$HMAC_{fail_{zone}} = \begin{matrix} & CCMP_{p_{value}} & CCMP_{1-P_{value}} \\ F_{ZA} & 07 & 05 \\ CF_Z & 03 & 06 \\ F_{ZB} & 11 & 10 \end{matrix} \quad (15)$$

$$CCMP_{pass_{zone}} = \begin{matrix} & CCMP_{p_{value}} & CCMP_{1-P_{value}} \\ T_Z & 100 & 95 \\ I_Z & 30 & 32 \\ S_Z & 86 & 86 \\ GE_Z & 12 & 10 \end{matrix} \quad (16)$$

$$HMAC_{pass_{zone}} = \begin{matrix} & CCMP_{p_{value}} & CCMP_{1-P_{value}} \\ T_Z & 67 & 80 \\ I_Z & 57 & 45 \\ S_Z & 75 & 47 \\ GE_Z & 07 & 08 \end{matrix} \quad (17)$$

Copyright © 2020 MECS

From Eq.(14) and Eq.(15), it is observed that the computation result of matrix $CCMP_{FZ}$ is smaller than that of matrix $HMAC_{FZ}$. It means that CCMP has smaller number of p_{values} and $1-p_{values}$ in all fall short zones in comparison to CBC-HMAC. Similarly, it is clear from Eq. (16) and Eq. (17) that computation of matrix $CCMP_{pass_{zone}}$ is much higher than that of $HMAC_{pass_{zone}}$. It means that the p_{values} and $1-p_{values}$ of all pass zones for CCMP are very high in comparison to that CBC-HMAC. Hence, it can be easily concluded that CCMP has lower number of p_{values} and $1-p_{values}$ in all fall short zones in comparison to CBC-HMAC whereas CCMP has higher number of p_{values} and $1-p_{values}$ in all pass zones in comparison to that CBC-HMAC.

The mean and standard deviation of p_{values} and $1-p_{values}$ for all fall short zones and all pass zones can also help in comparing the performance of CCMP and CBC-HMAC techniques. Here, following finishing rules (FRs) will be used to compare the performance:

FR_1: The technique having highest value of average mean and lowest value of average standard deviation for all pass zones will be considered as the best technique.

FR_2: The technique having lowest value of average mean and highest value of average standard deviation for all fall short zones will be considered as the best technique.

The values of mean and standard deviation for fall short zones and pass zones can be calculated using formulae of Eq.(18), Eq.(19), Eq.(20), Eq.(21) and Eq.(22).

$$\left\{\text{Mean of CCMP}_{\text{fail}_{\text{zones}}}^{\text{p}_{\text{values}}\text{ and }1-\text{p}_{\text{values}}}\right\} = \frac{[(\text{CCMP}_{\text{F}_{\text{ZA}}}^{\text{p}_{\text{values}}} + \text{CCMP}_{\text{CF}_{\text{Z}}}^{\text{p}_{\text{values}}} + \text{CCMP}_{\text{F}_{\text{ZB}}}^{\text{p}_{\text{values}}}) + (\text{CCMP}_{\text{F}_{\text{ZA}}}^{1-\text{p}_{\text{values}}} + \text{CCMP}_{\text{CF}_{\text{Z}}}^{1-\text{p}_{\text{values}}} + \text{CCMP}_{\text{F}_{\text{ZB}}}^{1-\text{p}_{\text{values}}})]}{6} \quad (18)$$

$$\left\{\text{Mean of HMAC}_{\text{fail}_{\text{zones}}}^{\text{p}_{\text{values}}\text{ and }1-\text{p}_{\text{values}}}\right\} = \frac{[(\text{HMAC}_{\text{F}_{\text{ZA}}}^{\text{p}_{\text{values}}} + \text{HMAC}_{\text{CF}_{\text{Z}}}^{\text{p}_{\text{values}}} + \text{HMAC}_{\text{F}_{\text{ZB}}}^{\text{p}_{\text{values}}}) + (\text{HMAC}_{\text{F}_{\text{ZA}}}^{1-\text{p}_{\text{values}}} + \text{HMAC}_{\text{CF}_{\text{Z}}}^{1-\text{p}_{\text{values}}} + \text{HMAC}_{\text{F}_{\text{ZB}}}^{1-\text{p}_{\text{values}}})]}{6} \quad (19)$$

$$\left\{\text{Mean of CCMP}_{\text{pass}_{\text{zones}}}^{\text{p}_{\text{values}}\text{ and }1-\text{p}_{\text{values}}}\right\} = \frac{[(\text{CCMP}_{\text{T}_{\text{Z}}}^{\text{p}_{\text{values}}} + \text{CCMP}_{\text{I}_{\text{Z}}}^{\text{p}_{\text{values}}} + \text{CCMP}_{\text{S}_{\text{Z}}}^{\text{p}_{\text{values}}} + \text{CCMP}_{\text{GE}_{\text{Z}}}^{\text{p}_{\text{values}}}) + (\text{CCMP}_{\text{T}_{\text{Z}}}^{1-\text{p}_{\text{values}}} + \text{CCMP}_{\text{I}_{\text{Z}}}^{1-\text{p}_{\text{values}}} + \text{CCMP}_{\text{GE}_{\text{Z}}}^{1-\text{p}_{\text{values}}})]}{8} \quad (20)$$

$$\left\{\text{Mean of HMAC}_{\text{pass}_{\text{zones}}}^{\text{p}_{\text{values}}\text{ and }1-\text{p}_{\text{values}}}\right\} = \frac{[(\text{HMAC}_{\text{T}_{\text{Z}}}^{\text{p}_{\text{values}}} + \text{HMAC}_{\text{I}_{\text{Z}}}^{\text{p}_{\text{values}}} + \text{HMAC}_{\text{S}_{\text{Z}}}^{\text{p}_{\text{values}}} + \text{HMAC}_{\text{GE}_{\text{Z}}}^{\text{p}_{\text{values}}}) + (\text{HMAC}_{\text{T}_{\text{Z}}}^{1-\text{p}_{\text{values}}} + \text{HMAC}_{\text{I}_{\text{Z}}}^{1-\text{p}_{\text{values}}} + \text{HMAC}_{\text{GE}_{\text{Z}}}^{1-\text{p}_{\text{values}}})]}{8} \quad (21)$$

$$\{\text{Standard Deviation of CCMP and HMAC }\} = \sqrt{\frac{\sum_{\text{i}=1}^{\text{N}}(\text{x}_{\text{i}}-\bar{\text{x}})^2}{\text{N}-1}} \quad (22)$$

The calculated values of mean and standard deviations for different *fall short zones* and *pass zones* of CCMP and HMAC using Eq.(18), Eq.(19), Eq.(20), Eq.(21) and Eq.(22) for fig. 9, fig. 10, fig, 11, and fig. 12 are presented in table 3. Therefore, the data sources of table 3 are the computed values of mean and standard deviations of p_{values} and $1-p_{values}$ obtained for different *fall short zones* and *pass zones* of CCMP and HMAC using Eq.(18), Eq.(19), Eq.(20), Eq.(21), and Eq.(22) for fig. 9, fig. 10, fig, 11, and fig. 12.

After comparing mean and standard deviation of all *pass* and *fall short* zones using table 3 and Eq.(18) to Eq.(22) following observations were recorded:

Observation 1: The CCMP technique has significantly lower number of $Mean_{p_{values}}$ and $Mean_{1-p_{values}}$ in all fail zones inclusively in comparison to that of CBC-HMAC.

Observation 2: The CCMP technique has considerably higher number of $Mean_{p_{values}}$ and $Mean_{1-p_{values}}$ in all pass zones in comparison to that of CBC-HMAC.

Observation 3: The average of standard deviations for p_{values} and $1-p_{values}$ of CCMP technique in all fail zones inclusively is much higher than that of CBC-HMAC.

Observation 4: The average of standard deviations for p_{values} and $1-p_{values}$ of CCMP technique in all pass zones inclusively is appreciably smaller than that of CBC-HMAC.

Therefore, on the basis of finishing rules (*FR_1* to *FR_2*), *Null Assumption*, *Alternate Assumption*, *Observation 1*, *Observation 2*, *Observation 3*, and *Observation 4* it is clearly proved that encoding and decoding performance of CCMP is a far better than CBC-HMAC.

Table 3. Computation results of mean and standard deviations for CCMP and HMAC techniques

	$CCMP_{pass_{zones}}$	$HMAC_{pass_{zones}}$	$CCMP_{fail_{zones}}$	$HMAC_{fail_{zones}}$
Mean of p_{values}	57.00	51.50	4.66	7.00
Mean of $1-p_{values}$	55.75	45.00	6.33	7.00
Average of Mean for p_{values} and $1-p_{values}$	**56.38 (High)**	**48.25 (Low)**	**5.50 (Low)**	**7.00 (High)**
Standard Deviation of p_{values}	43.71	30.52	4.73	4.00
Standard Deviation of $1-p_{values}$	702.50	866.29	2.54	2.69
Average of standard deviation for p_{values} and $1-p_{values}$	**373.11 (Low)**	**448.41 (High)**	**3.64 (High)**	**3.35 (Low)**

In cloud computing and Internet of Things (IoT) related communication systems the end users communicate with each other by sending and receiving messages. These messages are transmitted in encoded format and before displaying data the receivers system decodes it. Therefore, the decoded data is always displayed on the screen. In this research work the author has proved on the basis of mean and standard deviations of p_{values} and $1-p_{values}$ in different zones that CCMP is a far superior PRF than that of CBC-HMAC. Hence, on the basis of these comparisons and detailed analysis of results the author recommends that the use of CCMP based communication systems will be advantageous, speedy, efficient and secure for sending and receiving messages through internets of things (IoT) and other cloud computing systems [55] [56].

5. Conclusions

In order to conduct statistical and geometric study of CCMP and CBC-HMAC, the NIST test tool [40] and DIEHARD geometric study instruments [48] were tolerably examined and an knowledgeable choice was decided to apply DIEHARD because of its straightforwardness, exactness of outcome, and capacity to route huge files without using towering computing influence. The accurate geometric analysis was conducted on the basis of inference rule (IR_1 to IR_7), *Null Assumption*, *Alternate Assumption*, and finishing rules (FR_1 to FR_4) for computing average mean and standard deviations of p_{values} and $1-p_{values}$ for all fall short and pass zones.

The investigations of this research work shows that CCMP is efficient enough in the ensuing zones like problem of parameterization, effectiveness, and protection measures. The proposed CCMP based representations is able to handle robustness situations and cases accurately and efficiently. The proposed analysis provides us very clear evidences that the PRF of CCMP is a superior and secure in contrast to that of CBC-HMAC. Hence, the author proposes in this research work that CCMP based communication techniques should be preferred in all internets of things (IoT) and cloud computing related communication systems in order to further improve the accuracy, efficiency, security and reliability of cloud-IoT integrated distributive computing system. The author observed that the PRF of CCMP is better than CBC-HMAC. The performance of CCMP based systems can be further enhanced in future by accumulating random encoding and decoding capabilities in the cloud-IoT enabled distributive computing systems.

References

[1] Tao Feng, Yun Cheng, "Comprehensive Research and Application of Cloud Computing in Enterprises", International Journal of Grid Distribution Computing, Vol.7, No. 6, pp.191- 200, 2014.
[2] http://cloudcomputing.sys-con.com/node/612375/print Accessed on May 5, 2016.

[3] http://www.nist.gov/itl/cloud/ Accessed on May 6, 2016.
[4] Mohammad Sajid, Zahid Raza, "Cloud Computing: Issues & Challenges", International Conference on Cloud, Big Data and Trust, pp.35-41, 2013.
[5] Peter Mell, Timothy Grance, "The NIST Definition of Cloud Computing", U.S. Department of Commerce, National Institute of Standards and Technology, pp. 1-3, 2011.
[6] The Stationery Office, "The Official Introduction to the ITIL Service Lifecycle", OGC (Office of Government Commerce), United Kingdom, pp. 1-172, 2007.
[7] J. Van Bon, A. van der Veen, "Foundations of IT Service Management based on ITIL", Vol. 3, Van Haren Publishing, Zaltbommel, 2007.
[8] M. Miller, "Cloud Computing: Web based applications that change the way you work and collaborate online", Que Publication, 2008.
[9] D. C. Plummer, D. Smith, T. J. Bittman, D. W. Cearley, D. J. Cappuccio, D. Scott, R. Kumar, B. Robertson, "Gartner highlights five attributes of cloud computing, Gartner Report", Vol. G00167182, pp. 1 5, 2009.
[10] R. Buyya, C. S. Yeo, S Venugopal, "Market oriented cloud computing: Vision, hype, and reality for delivering IT services as computing utilities", in Proceedings of the 10th IEEE International Conference on High Performance Computing and Communications (HPCC 2008, IEEE CS Press, Los Alamitos, CA, USA), Dalian, China, September 25-27, pp. 1-9, 2008.
[11] D. Alger, "Build the Best Data Center Facility for Your Business", Cisco Press, Indianapolis, USA, June 2005.
[12] P. Mell, T. Grance, "The NIST Definition of Cloud Computing", version 15, National Institute of standards and Technology (NIST), Information Technology Laboratory, pp. 1- 3, 2009. Online Available On: www.csrc.nist.gov , Last Accessed On: July 21, 2017.
[13] Peter Mell. (2011) 'The NIST Definition of Cloud, Reports on Computer Systems Technology", pp. 1-7, 2011. Online Available On: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf , Last Accessed On: July 21, 2017.
[14] D.K. Mishra. (Sept.2010) 'Tutorial: Secure Multiparty Computation for Cloud Computing Paradigm", Second International Conference on Computational Intelligence, Modeling and Simulation, pp. 1-6, 2010.
[15] I. Foster, C. Kesselmann, "The Grid: Blueprint for a New Computing Infrastructure", Morgan Kaufmann Publishers, USA, 1999.
[16] http://www.druva.com/documents/Druva-inSync-Security-Q115-R54-10062.pdf. Lat Accessed on: May 5, 2017.
[17] J. Barr, A. Narin, and J. Varia, "Building Fault-Tolerant Applications on AWS", Amazon Web Services, pp.1-15, 2011.
[18] U. Khalid, A. Ghafoor, M. Irum and M. Awais Shibli, "Cloud Based Secure and Privacy Enhanced Authentication and Authorization Protocol", Procedia Computer Science, Vol.22, pp. 680-688, 2013.
[19] D. Zissis, D. Lekkas, "Addressing Cloud Computing Security Issues", Future Generation Computer Systems, Vol. 28, No. 3, pp.583-592, 2012.
[20] D. W. Chadwick, K. Fatema, "A privacy preserving authorization system for the Cloud", Journal of Computer and System Sciences, Vol. 78, No. 5, pp. 1359-1373, 2012.
[21] A. Saldhana, R. Marian, A. Barbir, S. A. Jabbar, "OASIS Cloud Authorization (CloudAuthZ)", International Journal of Multimedia and Ubiquitous Engineering, Vol. 9, No. 9, pp. 81-90, 2014.
[22] http://www.vmware.com/files/pdf/partners/vmware-public-cloud-security-wp.pdf?src=vcld-2012-1-blog-PCSA%20whitepaper-ex-41 Last Accessed on May 5, 2017.
[23] http://www.dell.com/learn/us/en/04/campaigns/data-protection, (2013-11-06) Last Accessed on: May 5, 2017.
[24] Wood K, Pereira E. (Nov.2010) "An Investigation into Cloud Configuration and Security", International Conference for Internet Technology and Secured Transactions, pp. 1-6. 2010.
[25] http://searchsecurity.techtarget.com/definition/authentication-authorization-and-accounting Last Accessed On: May 5, 2017.
[26] Idris Ahmed, Anne James, Dhananjay Singh, "Critical analysis of counter mode with cipher block chain message authentication mode protocol—CCMP", Security and communication Networks, Vol. 7, No. 2, pp. 293–308, 2013.
[27] M. Hogan, F. Liu, A. Sokol, J. Tong, NIST Cloud Computing Standards Roadmap – Version 1.0, Natl. Inst. Stand. Technol. Spec. Publ. 500- 291, pp. 1-63, 2011.
[28] R. Ahuja "SLA Based Scheduler for Cloud storage and Computational Services", International Conference on Computational Science and Applications (ICCSA), pp.258-262, 2011.
[29] A. Albeshri, W. Caelli, "Mutual Protection in a Cloud Computing Environment", 12th IEEE International Conference on High performance Computing and Communications (HPCC), pp. 641-646, 2010.
[30] Bellare, M., Kohno, T., Namprempre, C. "Authenticated encryption in SSH: provably fixing the SSH binary packet protocol". In Altari, V., Jajodia, S., and Sandhu, R. (Eds.) Proceedings of 9th Annual Conference on Computer and Communications Security – CCS 2002,held 18 – 22 November 2002 in Washington, USA. New York: ACM Publication, pp1-11, 2002.
[31] Bellare, M., Kilian, J., Rogaway, P. "The Security of the Cipher Block Chaining Message Authentication Code", Journal of Computer and System Science, Vol. 61, No. 3, pp. 362-399, 2001.
[32] Black, J., Rogaway, P. "A suggestion for Handling Arbitrary-Length Messages with the CBC-MAC". In Bellare, M. (Ed.) Proceedings of 20th Annual International Conference of Advances in Cryptology – CRYPTO 2000, Lecture Notes in Computer Science 1880, held 20-24 August 2000 in Santa Barbara, USA. Berlin: Springer, pp 197 – 215.
[33] Rogaway, P. and Black, J. "A Block-Cipher Mode of Operation for Parallelizable Message Authentication". In Knudsen, L. R. (Ed.) Proceedings of the International Conference on Theory and Applications of Cryptographic Techniques, Advances in Cryptology - EUROCRYPT 2002, Lecture Notes in Computer Science 2332, held 28 April -2 May 2002 in Amsterdam, Holland. Berlin: Springer, pp 384-397.
[34] Caballero, J., Yin, H., Liang, Z., and Song, D. "Polyglot: automatic extraction of protocol message format using dynamic binary analysis". In Ning, P. (Ed.) Proceedings of the 14th ACM Conference on Computer and Communications Security - CCS 2007, held 28-31 October 2007 in Whistler, Canada. New York: ACM Publication, pp 317-329, 2007.
[35] Robert, A. E., Manivasagam, G., Sasirekha, N., Hemalatha, M. "Reverse Engineering for Malicious Code Behaviour Analysis using Virtual Security Patching". International Journal of Computer Applications, Vol 26, issue 4, pp. 41-45, 2011.

[36] Alani, M. M. "Testing Randomness of Block-Ciphers using Diehard Test", International Journal of Computer Science and Network Security, Vol 10, No. 4, pp 53-57, 2010.
[37] Whiting, D., Housley, R., and Ferguson, N. "AES Encryption & Authentication Using CTR Mode & CBC-MAC". http://csrc.nist.gov/groups/ST/toolkit/BCM/current_modes.html#03. (Online available May 6, 2017)
[38] Whiting, D., Housley, R., and Ferguson, N. "AES Encryption & Authentication Using CTR Mode & CBC-MAC". http://csrc.nist.gov/groups/ST/toolkit/BCM/current_modes.html#03 (Online available May 6, 2017)
[39] Whiting, D., Housley, R., and Ferguson, N. "AES Encryption & Authentication Using CTR Mode & CBC-MAC http://csrc.nist.gov/groups/ST/toolkit/BCM/current_modes.html#03 (Online available On: May 6, 2017).
[40] NIST Publication 2001 "Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications". http://csrc.nist.gov/publications/nistpubs/800-22/sp-800-22-051501.pdf (Online available May 6, 2017).
[41] Johnson, D. H. "The Insignificance of Statistical Significance Testing". The Journal of Wildlife Management, Vol. 63, No. 3, pp 763-772, 1999.
[42] Masson, M. E. J., and Loftus, G. R. "Using confidence intervals for graphically based data interpretation", Canadian Journal of Experimental Psychology, Vol. 57, No. 3, pp. 203, 2003.
[43] Impagliazzo, R., and Naor, M. "Efficient Cryptographic Schemes Provable as Secure as Subset Sum". Journal of Cryptology, Vol. 9, No. 4, pp 199-216, 1986.
[44] Kenny, C. "Random Number Generators: An evaluation and comparison of Random.org and some commonly used generators". http://www.random.org/analysis/Analysis2005.pdf > (Online available May 6, 2017)
[45] Lipmaa, H., Rogaway, P., and Wagner, D. "Counter Mode Encryption". http://www.cs.ucdavis.edu/research/tech-reports (Online available May 6, 2017)
[46] Marsaglia, G. "Diehard Battery of Statistical Test". http://stat.fsu.edu/~geo/diehard.html (Online available May 6, 2017)
[47] S. Almulla, Y-Y Chon, "Cloud Computing Security management", 2nd International Conference On Engineering Systems Management and Its Applications, pp.1-7, 2010.
[48] I. Ahmed, A. James, D. Singh, "Critical analysis of counter mode with cipher block chain message authentication mode protocol—CCMP", Security and Communication Networks, Vol. 7, No. 2, pp. 293–308, 2014.
[49] Security Guide for Critical Area s of Focus in Cloud Computing V3.0 https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf Last Accessed on: July 2017
[50] F. Khodadadi, R.N. Calheiros, R. Buyya, "A Data-Centric Framework for Development and Deployment of Internet of Things Applications in Clouds", Proc. of the 10th IEEE International Conference on Intelligent Sensors, Sensor Networks and Information **Process**ing (ISSNIP 2015), Singapore, April 7-9, pp. 1-6, 2015.
[51] A. M. Alberti, V.H.O. F.ernandes, M.A.F. Casaroli, L.H.D. Oliveira, F. M.P. Junior, D.Singh, "A Nova Genesis Proxy/Gateway/Controller for Open Flow Software Defined Networks", in a workshop of Man SDN/NFV, 10th International Conference on Network and Service Management (CNSM 2014) in Rio de Janeiro, Brazil, November 17-21, pp. 1-5, 2014.
[52] D. Singh "Developing an Architecture: Scalability, Mobility, Control, and Isolation on Future Internet Services", Second International Conference on Advances in Computing, Communications and Informatics (ICACCI), Mysore, India, pp. 1873-1877, 2013.
[53] Singh Irish, Mishra K. N., A. Alberti, D. Singh, A. Jara, 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, pp. 301 -305, 2015.
[54] Kamta Nath Mishra, A Novel Mechanism for Cloud Data Management in Distributed Environment, *A Book On Data Intensive Computing Applications for Big Data, IOS Press USA*, pp. 386-413, January, 2018.

Authors' Profiles

Dr. Kamta Nath Mishra
Department of Computer Science & Engineering
Birla Institute of Technology, Jharkhand, India, Pin: 814142;
Phone +91-9695052989

Short Biography: Dr. Kamta Nath Mishra was born on August 15, 1973 in Kushinagar district of Uttar Pradesh, INDIA. He received his Bachelor of Science (B.Sc., Maths) degree from University of Gorakhpur, INDIA, in 1992, and Master of Computer Application (MCA) degree from Madan Mohan Malviya Engineering College (Currently MMMUT), Gorakhpur, U. P., INDIA in 1996. Dr. Mishra completed his M.Tech. (Software Systems) degree from Birla Institute of Technology and Science (BITS) Pilani, INDIA in 2003 and Ph.D. (Engg.) from CSE department of B.I.T. Mesra – INDIA, in May 2015.

Dr. Mishra has more than twenty years of teaching and research experience. Currently, he is working as a Senior Faculty Member at Dept. of CS&E, B.I.T. Mesra, Ranchi, INDIA since August 2009; He has worked as a faculty member in the department of Computer Science, Joint programme of Michigan State University USA and University of Sebha, LIBYA, from October 2006 to July 2009. He was a senior lecturer at B.I.T. Mesra, (Noida Campus) from July 2004 to September 2006. Dr. Mishra has worked as a senior project engineer from September 2003 to June 2004 and project engineer from September 2000 to August 2003, in Centre for Development of Advanced Computing (Ministry of Communication & IT, Govt. of India) Noida, Uttar Pradesh. Before joining CDAC, Dr. Mishra worked as a lecturer in CS&E department at Krishna Institute of Engineering & Technology (KIET), Ghaziabad, INDIA, from July 1998 to August 2000.

Dr. Mishra has published two books, ten book chapters (Springer, IGI Global, Elsevier) and more than thirty research articles in journals and conferences of international repute. His research interest includes Biometric Systems, Image Processing, Analysis of Algorithms, Cloud Computing, Smart Society Computations, and Distributed Cloud Computing. Dr. Mishra is a professional member of IEEE Biometric Society USA, and ACM, USA.

How to cite this paper: Kamta Nath Mishra, "A Proficient Mechanism for Cloud Security Supervision in Distributive Computing Environment", International Journal of Computer Network and Information Security(IJCNIS), Vol.12, No.6, pp.57-77, 2020. DOI: 10.5815/ijcnis.2020.06.05

Copyright © 2020 MECS