International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-11, September 2019

An Invincible Rudimentary Architecture for Data Security in Cloud Environment Using Multi Cloud

N. Velmurugan, S. Godfrey Winster

Abstract:- ***Cloud is a distributed access of shared pool of resources that can provide the efficient service on demand basics to cloud user by the service providers. The important functions of cloud computing are storage and computation. The cloud user can use the cloud functions without any computing resources. Because of the popularity of cloud computing, providing security to the stored data is a major concern. In the literature, there are various works which have been proposed to provide the efficient security to the stored data in cloud environment. This paper provides the details of need of security in cloud environment, various categories of security threats, mechanisms, cloud architecture, multi-cloud and various security algorithms in detailed manner. The main attention of this paper is to point out the works on security in cloud computing, show the proposed architecute of multi cloud instead of single cloud and the way for the future work for the efficient design of cloud secure service system.***

Index Terms : Cloud computing, Cloud security, Data Security, Security algorithms, Confidentiality, Data Protection, Data Privacy

I. INTRODUCTION

Cloud computing is a various service such as software, software development platforms, hardware, storage and network facility through the internet [1]. On-demand self-service, broad network access, resource pooling, rapid elasticity and measured service are characteristics of the cloud. Services of cloud are Software, Platform and Infrastructure as a Service which is termed as SaaS, PaaS, IaaS respectively. Cloud models are private cloud, public cloud, Community cloud, Hybrid cloud. Zhao et al. have proposed five models of cloud computing obstacles. Separation, availability, migration, tunnel and encryption are the models shown by them [2]. Cloud provides have two functions such as storage of data and computations. In cloud, the consumers of cloud services not require any computing resources but they can retrive the data and to impute the works through the internet. During the data retrivel, storage and computing, the end users unable to understand the storage of data and which machine executes their computing tasks. Data protection, privacy and more security are the important elements for getting user's faith and successful of cloud technology in data storage. A lot of techniques to secure data have been suggested to overcome the secuity issues in cloud environment. However, related to data protection techniques are require to be enhanced [3]. Security is an encomposise of confidentiality, integrity and data availability.

Manuscript published on 30 September 2019.
*****Correspondence Author(s)
* **N. Velmurugan,** Research Scholar, Saveetha School of Engineering, SIMATS, Chennai, India.
S. Godfrey Winster, Professor, CSE, Saveetha Engineering College, Chennai, India.

the users to be less dependent on the client system and provides an architecture to upload the data to cloud that can be shared by multiple users and also provide security through authentication of the end user by the service provider. There are lot of advantages of cloud computing technology. The important advantages of cloud computing are follows lower computing cost for comsumers, lower IT infrastructure cost, less maintenance cost, reducing software cost, direct software updates, increased computing power and extented storage capacity. But require a constant high speed internet connection. The stored data might not be secure. The rudimentary idea is to use more clouds at the similar time to mitigate the risks of malicious data manipulation, disclosure, and process tampering [4]. Zahir Tari gives an overview of novel challenges, opportunities, and solutions in cloud security. He has identified some important area to be secure such as virtual infrastructures, user data, storage of big data and access mechanism. The guidelines about the new threats and vulnerabilities are discussed. The remaining division of this paper is ordered as follows. Section 2 discusses background works related to security categories, levels, algorithms, architectures, standards, attacks etc. They provides the analysis of security algorithms and tabled with different characteristics of each algorithm. Section 3 describes proposed multi cloud architectures for different file fomats 4 results and proposed architecture sources 5 conclusion and future research directions.

II. BACKGROUND

A. Security Architecture / Auditing

Khaled et al. have proposed security overlay architectures called Intrusion Detection Systems (IDSs) which monitoring the traffic in a given cloud network [5]. Lan et al. have proposed a RBAC based cloud storage architecture which has the characteristics of constant size, encrypted text and decryption key. Lan concluded as encryption and decryption are efficient on client side. RBAC architecture consists of public or private cloud, user, role of manager, owner and administrator [6]. Edward proposed architecture for securing cloud architecture using the following components and concepts. The components are identity and access, service gateways and concepts are user account security, user separation, content distribution, virtualized security capabilities etc. Edward G. have explained the practical approaches to secure the data storage in cloud, infrastructure and services. The services are includes private cloud with enterprise perimeters, public cloud with service gateways, encryption, session containers, cloud brokers and runtime security virtualization. They safeguards the private cloud, firewall, IDPS (Intrusion Detection / Prevention System), DLP (Data Loss

Prevention), encryption, SIEM (Security Information Event Management) analytics. The security controls in public cloud services includes service provider perimeter, user account security, user separation, content distribution and virtualized security capabilities [7]. Several Security Reference Architecture (SRA) are available in IBM, MS, Amazon, VMware, Oracle and so on. Standard SRA is Payment Card Industry (PCI) - compliant cloud reference architecture, Data Security Standard (DSS) given by Eduardo B. Fernandez et al. [8].

B. Security Categories / Levels

Richard Chow et al. have categorized the security as traditional, availability, third party data control. Traditional security includes VM (Virtual Machine) level attacks, authentication and authorization, vulnerabilities, network attacks, forensics. Availability includes time during in operation, failure and computational reliability. Mazhar Ali et al., proposed the security issues are listed as communication, architectural level and contractual and legal issues. Communication level includes internet, protocol and sharing infrastructure, Architectural level includes virtualization, data storage, web application and Application Programming Interface (API) security and identity management and access control. Virtualization issues are such as VM escape, VM isolation, VM migration, VM rollback, hypervisor and VM sprawl. Data / storage issues are such as data privacy and integrity includes confidentiality, integrity and availability, data recovery vulnerability, unsuitable media sanitization, data backup recovery etc. Web application and API security issues are broken authentication, session management and cross site scripting (XSS) etc [9]. Chirag et al. have done a detailed survey on security problems in cloud computing and listed the security challenges in the cloud as vulnerabilities, threats and attacks. The vulnerabilities issues are available in OS Level, IP, unauthorized attacks and application and hypervisor based virtualization. Threats issues occur in business model, insecure interface and API, malicious insiders, shared technology, data loss and leakage and service hijacking. Attacks related issues are zombie (compromising valid user VM), service injection, virtualization, man-in-the middle, metadata spoofing, phishing and backdoor channel attack etc [10]. Issa et al. have discussed five cloud security categories such as global security, network security, access control, cloud infrastructure and data security. Security standards related issues are includes Service Level Agreements (SLA) in proper, lack of auditing etc., Network related issues are includes network firewalls, security configurations and protocol vulnerabilities. Access control related issues are includes account hijacking, service hijacking, malicious insiders, authentication mechanism, privileged user access and browser security. Cloud infrastructure related issues are includes insecure interface, QoS, server location and backup. Data related issues are includes data redundancy, leakage, loss, location, recovery, privacy and protection [11].Azua et al. have identified the importance of security, compliance business risks such as multi-tenancy, automation, standardization, authentication & authorization, device endpoints, the concentration of value, and human factors. The result of the experts in the order of higher risk to lower risk as follows: human factors, massive amount of data, end points, authentication & authorization, standardization, automation, multi-tenancy, hypervisor. The result of the survey is that, data is in the order of lower risk to higher risk as follows: automation, standardization, authentication & authorization, hypervisor, massive amount of data, human factors, end points, multi-tenancy[12]. Nelson et al. have analysed the security categories and the results are identified, classified, organized and quantified the main security concerns and solution by ENISA (European Network and Information Security Agency), the Cloud Security Alliance (CSA), NIST (National Institute of Standards and Technology). They have listed the seven security categories such as network, interfaces, virtualization, governance, issues of compliance, legal and data security [13]. Hashizume et al. have identified the main vulnerabilities in cloud security standards, data security, trusts, security requirements, SaaS, PaaS and IaaS. They classified, analysed the list of vulnerabilities, threats focused on cloud computing and possible solutions and mechanisms [14]. Hsin-Yi et al. focussed on data security and virtual machine security. Data security is providing listed as confidentiality, integrity, availability and security management which critical for cloud security at user data level. Virtual machine (VM) vulnerabilities are VM hopping, VM diversity, VM mobility and VM denial of service [15]. Xuexiu et al. have proposed a security assessment system and protection layers. Security assessment systems are includes internet access area, core area, safety management area, internal user area, cloud service and data area and other system areas. Protection layers are includes physical, network, host, abstract resource, software, application and data security [16]. Dana et al. have listed the cloud portability taxonomy, requirements, various approaches and research agenda. They listed open-source libraries, open-source tool or service and implementations of semantic concept for supporting to researcher and academicians [17]. Ashish Singh et al. have addressed the cloud security concepts, cloud architecture framework, cloud technologies, threats, and attacks. They listed the following threats such as service delivery, violent use of cloud, insecure interface, data leakage and loss and shared technology issues [18]. Minhaj Ahmad Khan have identified attacks on network, virtual machine, storage and applications. They generated automated protection systems such as ACARM, Suricata, OSSEC, Snort, NIDES, Sagan, Samhain and Fail2ban [19].Anna Kobusinska et al, have listed the areas to be more considered in the cloud security like confidentiality, data verification, authorization, mining, secure communication and computations. Fahad F. Alruwaili et al, have analyzed on the following areas such as Information Security, Privacy, and Compliance Policy, Confidentiality, Integrity, Availability, Privacy and Compliance. Antivirus, Authentication, Backup, Disaster recovery, Encryption and Updates are listed by the dependencies on confidentiality in the security of cloud [20].

Amir Taherkordi et al, discussed the security in cloud and it sub areas, research challenges and future directions. They completed the survey on architecture, resource management, data management, application domains, privacy, confidentiality, and interoperability. One of the major challenges was noted as privacy and confidentiality by them [21].

C. Security Mehanism / Policy

Malina et al., have analysed current situation privacy preserving solutions provides for cloud services. They also proposed a unique security solution for cloud services which group signatures based anonymous authentication [22]. John Steven et al., have suggested that security must extended up to infrastructure (computing, network, and storage) and infostructure (applications, data and services), metastructure (protocols of internet, internet access, gateway etc.). Steven et al. have discussed about four technology patterns such as gateways, monitoring, Security Token Services (STSs) and Policy Enforcement Points (PEPs). Ouedraogo et al. have listed the overview of cloud related threats and solutions based on cloud security alliance for establishing a improved security transparency between a cloud provider (CSP) and a cloud consumer (CSC) [23]. Jungwoo Ryoo et al, have discussed auditing challenges and approaches and conclude the cloud auditing standards which are includes Service Organization Control (SOC), NIST, CSA, PCI & DSS, ISO etc [24].

Kristian et al. have proposed pattern based method for classifying and analysing of threats, threat actions, cloud elements and stakeholder. The pattern based method provides dependability checks, validating privacy requirements and threat analysis, security integration and legal compliance [25]. Antonios et al., has listed that policies, models and mechanisms of Access Controls (AC). A policy defined in high level as how and when a user can access a specific resource. AC policies defined in a system level as method is responsible for allowing or rejecting a user access a resource. AC model defined as apool of access control mechanism implementations, which are protecting support for system policies through a conceptual framework [26].

D. Security Algorithms

Various security techniques have been to provide the proposed a comparative analysis of the existing work done in integrity, availability of data and confidentiality. Comparative analysis of data security and privacy could help to know the efficiency of security in cloud. Darko et al. have proposed a new encryption system for cloud which is called homomorphic. The system allows us for manipulation on chipper text without knowing the private key and without decrypting that data. Also partially and fully homomorphic encryption system solved many privacy issues. Iram Ahmad et al. have listed the algorithms with the homomorphic properties and explained multiplicative and additive homomorphic encryption. They have proposed proxy re-encryption algorithm with uses the paillier and RSA cryptosystem [27]. Among them ABE, IBE, SHA are the popular security algorithms used for cloud security.

Attribute Based Encryption (ABE)

Vipul Goyal et al. have explained Attribute Based Encryption (ABE) and it was introduced by Sahai and Waters for encryption systems with high expressiveness. They have to encryption techniues. They are Cipher text-Policy Attribute Based Encryption (CP-ABE) and Key-Policy Attribute Based Encryption (KP-ABE). In Attribute Based Encryption (ABE) system, a user's keys and cipher texts are used for encryption and a particular key can decrypt a particular cipher text. This is done when match between the attributes of the cipher text and the user's key [28, 29].

Identity Based Encryption (IBE)

A. Shamir has proposed identity based scheme based on a public key cryptosystem. User can create public key using unique identification of user like email. Private key created from the public key by the third party. He also summarizes the differences between private key, public key, and identity based cryptosystems. Joonsang Baek et al. have proposed a scheme, sender can use receiver's email or IP address or digital image for encrypt a message. The receiver can obtained a private key from Private Key Generator (PKG) which can decrypt the encrypted text. An identity based encryption scheme has following algorithms: Setup, Extract, Encrypt, Decrypt [30 - 32].

Secure Hash Algorithm (SHA)

National Institute of Standards and Technology (NIST) have SHA-1 which was developed by the National Security Agency (NSA) as SHA-0. Secure hash algorithm based on the concept of hash function. The basic idea behind this, input as a variable length message and output as fixed length message which is known as hash or message-digest [33, 34].

Enhanced Advanced Encryption Standard (EAES)

Enhanced Advanced Encryption Standard is based on a substitution permutation network. Enhanced AES is commonly use block ciphers of size 256 bits. By design enhanced AES is faster than the conventional AES as the block size is two times higher. The four primitive functions are four sequences such as Sub Bytes, Shift Row, Mix Column and Add Round Key [35].

Algorithms listed in Table 1 and Table 2 [36] are the various security algorithms used in cloud infrastructure. Even though the above said algorithms provide the various security mechanisms which fail to address confidentiality, protection and privacy of the cloud data.

Categories of Security Issues

E. After analysis of the traditional system, we have categorized the Data Security Issues (DSI) such as data redundancy, leakage, loss, availability, recovery, confidentiality, protection, service availability, privacy and integrity. As per the Table 3, our bullet points are confidentiality (DSI5) has the security level in low, data protection (DSI6) has in low, and data privacy (DSI8) has in low. That is, DSI5, DSI6 and DSI8 are the most important issue in the cloud security. Hereafter the most important issues are termed as CPPD (Confidentiality, Protection and Privacy of Data). ***Loss of Data***

Cloud computing is reformatting the Information Technology field, at the same time creation of private or public or hybrid cloud is very simple with some technical knowledge and a purchase of a single server. In the Single cloud, data and process are maintained by a cloud provider leads to more security problems. In another words, data security like data integrity, privacy, protection, confidentiality are not concentrated by CSPs.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Sometimes cloud services lose the control on the data stored in data centres. The examples are for loss of data, privacy and confidentiality given in the next paragraph.
Data owners don't have the control on the data and whether the data is misusing or not. Single cloud data owners don't have the proof of data security and everything under the control of service provider. Data owners are unable to trust the cloud providers [37 - 39]. Data loss of user such as photos, contacts, calendars in Microsoft data center on October 2009. Microsoft has conceived after a year and unable recovered the mass of data [40]. Servers Ma.gnolia have a loss of data and unable to process of recovery, making the site basically dead [41]. For more data loss, refer to Cachinet and al [42]. Various Cloud providers used various technology or mechanism to solve the data privacy issues. But traditional mechanism, privacy risks and encryption techniques are limited. Garfinkel gives details of the loss of confidentiality in the Amazon Cloud service [43].

Tara Salman listed the attacks such as Signature wrapping attacks, when implemented on EC2 frameworks, EC2 system by virtualization of the IaaS, systems has reported an attack to Google Docs and some other attacks illustrated that major cloud provider have harsh security flaws in different cloud categories [44].

Considering the huge loss, we may suggest multi cloud or cloud of clouds or inter clouds instead of single cloud because storage, elasticity, privacy and confidentiality are highly secure in multiple Cloud Service Provider (CSP). Here we no need to depend the single CSP.

Multi cloud

This section describes the researcher's survey, introduction to multi-cloud environment, different security aspects using multi-cloud.

Multiple clouds have various names such as cloud of clouds, inter cloud, multi cloud, cloud federation, aggregated clouds, hybrid cloud, sky computing, multitier clouds, hierarchical clouds, cross cloud, cloud blueprint, cloud merge, fog computing, distributed clouds and so on.

Our aim is to provide architecture design guidance for data security with more than one cloud by a client or service. A multi cloud is able to distributing works to all cloud resources organized across multiple clouds by Pooyan. Ana Juan Ferrer et al., describes multi cloud is used to reduce the risks in service availability failures, low strength of confidentiality, corruption of data, loss of data protection and privacy and malicious insiders in single cloud service. Federated and multi cloud are two types of multiple clouds. In the first model, a concord between the various cloud service providers to use resources each other, while in the multi cloud model there is no such agreements [45, 46].

Rajkumar Buyya et al., concluded two approaches for cloud providers and client. The first approach is provider-centric and second is client-centric. In the first approach, cloud providers can share resources to fulfill the user requests and raises their profit. In the second approach, the client has the power of provisioning resources from multiple cloud providers and they can decide which provider to get the most benefit. Multi cloud applications are based on part of the second approach. [47]. Grozev et al., discussed about the two multi cloud models. The first model, consumer has awareness of one cloud and is not awareness of other cloud. In the second model, the consumer has awareness of the various clouds to create an agreement for services or resources. Multi cloud means multiple and independent clouds consumed by a consumer or a service [48].

Michele Ciavotta et al, work provides novel mathematical approach Mixed Integer Linear Program (MILP) which is based on queuing theory to find a strong multi cloud formation for a given software architecture. This approach is for reducing time and low costs application with QoS by providing search procedure to identify more and improved design alternatives. Victor Ion Munteanu et al, have listed the advantages of multi clouds includes optimize costs, improve QoS, avoid addiction on only one cloud service provider, ensure backup-ups to deal with disasters, deals the loading of service and resource, on-demand basis, services high availability, a multi cloud represents the usage of various and independent cloud service provider by a service [49]. Mohammed A. Al Zain et al. have addressed mechanisms that provides the solution for the security risks in cloud environment. Security of the single cloud and cloud storage, single cloud and multi clouds are deeply analysed. They concluded multi clouds have less attention in cloud security. They recommended that "cloud- of-clouds or multi clouds or inter clouds" as new technology for providing high security to cloud data.
Rajkumar Buyya et al., have listed the benefits of multi cloud and a depiction of aneka architecture. They have summarize the benefits of multi cloud that are summarized as to access to more viable prices, extreme availability and improved response time, fault tolerance and reliability, independent of cloud service provider and simplify the combination of on-premise with cloud resources. Rajkumar Buyya et. al., discussed about types of inter-cloud such as federation clouds and multi-cloud. A Federation cloud is set of cloud providers willingly interconnect their cloud infrastructures in order to share resources among each other. Federation cloud has two types which is peer to peer and centralized clouds. Multi cloud is a client or service uses more than one independent cloud, no volunteer interconnection and providers' infrastructures. Multi cloud has two types which is services and libraries [51].

Hai-Jia etal. described a technique for optimizing the splitting of file, distribute chunks of files inside a cluster availability and service ability. A file partitioning mechanism and procedure is used for to placement of each data block based on its size One can handle simultaneously using various cloud storage providers, each file divided in to several pieces using Redundant Residue Number System (RRNS). Storage method is categorized as store data over the cloud, store data over the cloud with RRNS and store data over the cloud with RRNS and encryption [52].

Dana Petcu have points out the importance of multi cloud and for individuals, cloud users and cloud providers. They listed software for multi cloud implements based on library software or servicesoftware. Library based software like jclouds, libcloud and SimpleCloud. The service-based software are classified in two categories such as hosted (RightScale, enStratus and Kaavo) and deployable (Aeolus, mOSAIC and Optimis). The Cloud brokers are working with SpotCloud, Scalr and Stratos [53].

We know very well about the four types of cloud deployment models. Here the multi cloud basic architecture is clearly illustrated in the Fig. 1. Fig.1 (a) is depict the multi-cloud architecture and Fig.1 (b) is example for multi-cloud which shows different cloud service provider. The user may store their file in different CSP. Here the duplicated data are stored and need more space. The more space is measured as number of CSP multiply by the size of the file. Rajeev Kumar Bedi et al, provides an analysis of various multi cloud applications for storage and to check their performance. This application includes battery, data, CPU usage and time consumed by mobile phone on WiFi. Deval Bhamare et al, presents an analytical model for the placement of service function chains (SFC) in multi cloud. The focus has been mainly on resource allocation, removing other important parameters such as delays to end users, Quality of Service and service level agreements (SLA). They try to optimize delay of service to SFC in a multi cloud along with constraints such as total deployment cost and SLAs [54]. Quanlu Zhang et al, proposed a new data hosting scheme has two key functions. One key function is selecting suitable clouds and to store data with low cost and confirmation of availability. Second key function is distributing data to access pattern and pricing of clouds. Data hosting scheme accommodates various pricing strategies, availability requirements and data access patterns. Fan Zhang et al, described an integrated skyline query processing method for growing number of cloud sites contained in the mashup applications. Faster skyline selection, low composition time, dataset distribution and resources combination declare the Quality of Service over various clouds. Using MapReduce paradigm, solved the skyline selection problem in mashup cloud platforms [55].
According to researcher's survey, if cloud environment is upgraded from single cloud to multi cloud architecture, cloud users may have low risk from security issues and to ensure the confidentiality, privacy protection of data in the cloud environment.

III. PROPOSED METHODOLOGY

According to multi-cloud architecture survey, we segregate the three categories of Multi-Cloud Architecture (MCA) as follows: 1. Multi-Cloud Architecture for Files (MCA-F), 2. Multi-Cloud Architecture for Bigdata (MCA-B), 3. Multi-Cloud Architecture for Secret Keys and Files (MCA-SF). Table 4 shows the files are categorized stored in the appropriate cloud. On the other hand, based on the file type, the files are stored in the particular cloud. In the Fig. 2, Text, Audio / Video, Database and Image files are stored in cloud A, cloud B, cloud C and cloud D respectively. Multi-Cloud Director (MCD) is used to identifying the type of file, transferring the file to appropriate cloud and maintaining the indexes. Fig.3 shows the multi-cloud environment for storage of Big Data. Based on the categories of Big Data, the cloud is selected and stored in the suitable cloud. On the other hand, based on the big data categories the files stored in the particular cloud. In the Fig. 3, Structured Data, Unstructured Data and Semi-structured Data are stored in cloud A, cloud B and cloud C respectively. MCD is used to identifying the type of data, transferring the data to appropriate cloud and maintaining the indexes. Fig.4 shows the secret key and file management in multi-cloud environment. On the other hand, the encryption, decryption keys and files are stored in appropriate cloud. In the Fig. 4, the keys and files are stored in cloud A and cloud B respectively. MCD is used to identifying the cloud to store the keys and files, transferring them in to appropriate cloud and maintaining the indexes. Using any one of the above prototype of multi cloud, we can propose lot of design for secure data with security mechanism.

IV.RESULTS

In the first result track, we have identified various security architectures, algorithms, categories and DSIs. And also risk levels for various issues of DSI are mentioned and considered for improving the most important security issues such as DSI5, DSI6 and DSI8. At the same time, we are changing the algorithms from past quadranscentennial for providing efficient security for the data in the cloud environment. In the second result track, Considering the huge loss, we may suggest multi cloud or cloud of clouds or inter clouds instead of single cloud because storage, elasticity, privacy and confidentiality are highly secure in multiple Cloud Service Provider (CSP). Here we no need to depend on the single CSP. In the Fig. 5, Flow graph shows creation of proposed multi cloud architecture for various file formats. This work process consists of security categories, mechanism, algorithms, basic architecture of cloud and multi cloud.

For the proposed architecture design, we consider the three categories are follows:

1. different formats of files such as text files, image files, audio & video files and database files.
2. Big data files such as structured, unstructured and semi structured files.
3. Secret keys and Files such as encryption and decryption key and respective files.

The above architectures are depicted in the figure 2 to 4. Fresh-Hand Algorithm will be developed in the future.

Table1. Security Algorithms – Symmetric

Algorithm Name/ Particulars	Data Encryption Standard(DES)	BLOWFISH	TWOFISH	RC5	3DES	AES
Year/Developer	1977 / IBM and recommended by NIST	1993 / Bruce Schneier	1998/ Bruce Schneier	1994 / Ron Rivest	1998	2000 / recommended by NIST
Key Size	64-bit	32-448 bits Variable length key	256-bit	2040-bit	192 bit	variable key

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Block size	64 bit fixed per Block	64 bits per Block	128 bits per Block	32, 64 or 128 bits per block	64 bits per Block	length of 128, 192, or 256 bits per Block
Security Level	Proven & Inadequate	Considered Secure	Considered Secure	Considered Secure	Considered Secure	Considered Secure
Advantages	Fast	Secure Shell Programs / throughput and power consumption	Fastest algorithm	Secure	3 times / increased the secure level	fast / large key size / secure
Disadvantages	insecure block cipher	Weak keys	Slow Speed	Speed is low	Slow/More time/throughput and power consumption	More rounds

Table 2. Security Algorithms – Asymmetric

Algorithm Name/ Particulars	RSA (Ron Rivest, Adi Shamir, and Leonard Adleman)	Digital Signature Algorithm (DSA)	Diffie-Hellman Key Exchange (D-H)	ECC (Elliptic Curve Cryptography)	MD5- (Message-Digest algorithm 5)
Year/ Developer	1977 / Rivest-Shamir-Adleman	1991 by NIST	1976 / Diffie-Hellman	1980 / Victor Miller	1992/ Ronald Rivest
Key Size	2048 / 3072-bit	1024-bit	3072-bit	2048-bit	128-bit hash
Methods	Private and Public Key	Entropy, secrecy, and random signature value	Key exchange	Points on a curve to define the public/private key pair	Hash value
Security Level	High	High	High	High	High
Advantages	Highly Secure	digital signatures	fast	smaller devices like cell phones	Higher bandwidth, checksum used to verify
Disadvantages	Speed is slow	Fixed sub group size	Key exchange through insecure	cipher test is large size	not support streaming for messages

Table 3. Categories of security issues

Categories of Data Security Issues	Data Security Issue (DSI) No.	Security level	Justification by author
Data redundancy	**DSI1**	High	More space available
Data leakage and loss	**DSI2**	High	Now a days, equipment having quality and maintained properly.
Data availability	**DSI3**	High	Depending upon the CSP, architecture its different.
Data recovery	**DSI4**	Low	Lot of software and hardware are available to recover.

Confidentiality	**DSI5**	Low	Authorization in not enough.
Data protection	**DSI6**	Low	More research going on in this area.
Service availability	**DSI7**	High	All this categories are good except last one.
Data privacy	**DSI8**	Low	More secure algorithms, high-end security architectures used. But still we unable to give high end privacy
Data Integrity	**DSI9**	High	This level also fine. Not required to more concentrations.

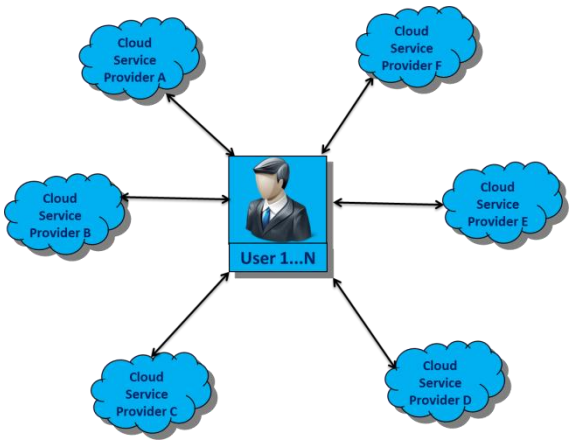

Fig.1 (a) Multi-Cloud

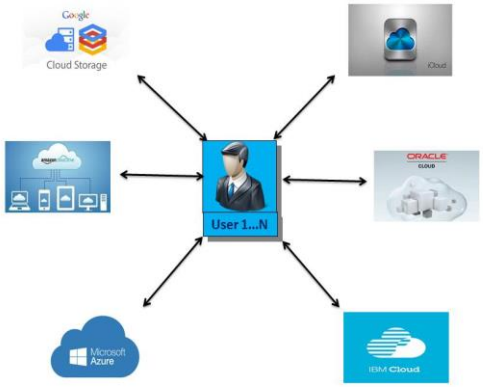

Fig.1 (b) Example for Multi-Cloud

Table 4 - Categories of files and respective multi clouds

Categories	Architecture Name	Type of source	Original content of file to be store
General Files	MCA-F	Different file types	Text, Image, Audio, Video files
Big data	MCA-B	Big data	Structured, Unstructured and Semi structured data
Secret Keys and Files	MCA-SF	Secret Keys	Encryption, Decryption keys and Files

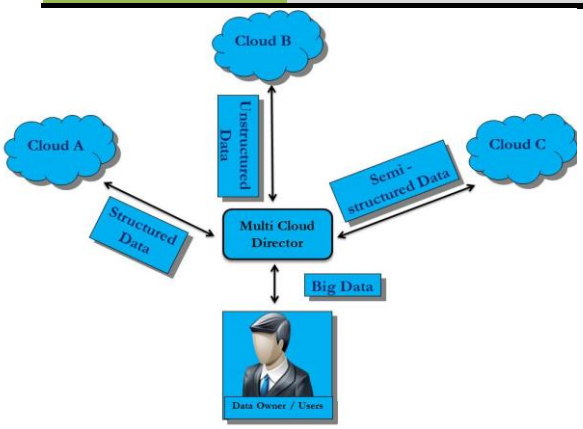

Fig.2 Multi-Cloud for Files

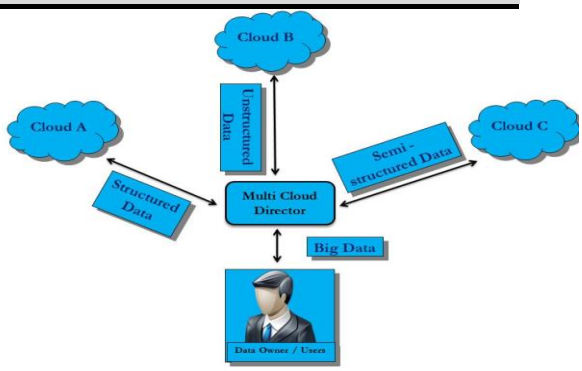

Fig.3 Multi-Cloud for Big data

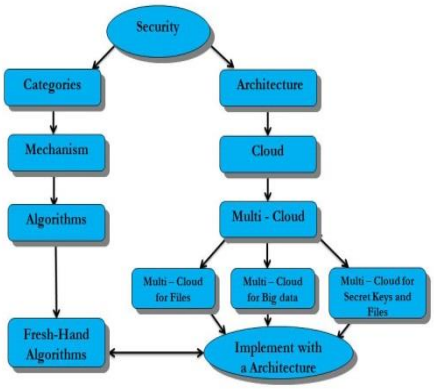

Fig.4 Multi-Cloud for Secret Keys and Files

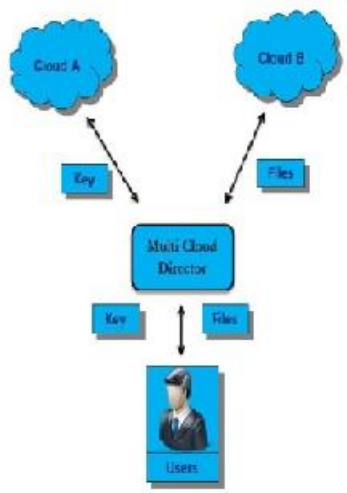

Fig.5 Flow graph of proposed work

V. CONCLUSION AND FUTURE RESEARCH DIRECTIONS

This paper provides the detailed analysis of traditional algorithms, categories of security issues, major security issues and the level of security in the cloud computing environment. Based an analysis, we found that the security level in Confidentiality, Protection and Privacy of Data (CPPD) are to be improved. From this survey, mostly the existing system algorithm and usage of the single cloud fails to CPPD efficiently. So recommend to use multi cloud architecture and develop a novel algorithm and mechanism for securing the data in the cloud environment. We finalized to focus on creating an innovative and first-handed algorithm which will be used in any one of the above multi cloud architecture. From the detailed analysis of the existing system, we suggest the following research area to be improved: first algorithms need to be innovative, second creating first-hand algorithms and third creating new design or pattern in multi cloud architecture to offer the high security for the data in the cloud environment.

REFERENCES

1. National Institute of Standard and Technology (NIST) Special Publication 800 – 145. Online http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
2. Gansen Zhao, Chunming Rong, Martin Gilje Jaatun, Frode Eika Sandnes, “Reference deployment models for eliminating user concerns on cloud security”, Springer, J Supercomput (2012) 61:337–352
3. Yunchuan Sun,Junsheng Zhang, Yongping Xiong, and Guangyu Zhu, “Data Security and Privacy in Cloud Computing”, International Journal of Distributed Sensor Networks, Hindawi Publishing Corporation Volume 2014, Article ID 190903, 9 pages.
4. A. Avi˘zienis, J. Laprie, B. Randell, and C. Landwehr, “Basic concepts and taxonomy of dependable and secure computing,” IEEE Transactions on Dependable and Secure Computing, vol. 1,no. 1, pp. 11–33, 2004..
5. Khaled Salah, Jose M. Alcaraz Calero, Sherali Zeadally, Sameera Al-Mulla and Mohammed Alzaabi, “Using Cloud Computing to Implement a Security Overlay Network”, IEEE Security & Privacy – 2013.
6. National Institute of Standard and Technology (NIST) Special Publication 800 – 145. Online http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
7. Gansen Zhao, Chunming Rong, Martin Gilje Jaatun, Frode Eika Sandnes, “Reference deployment models for eliminating user concerns on cloud security”, Springer, J Supercomput (2012) 61:337–352
8. Yunchuan Sun,Junsheng Zhang, Yongping Xiong, and Guangyu Zhu, “Data Security and Privacy in Cloud Computing”, International Journal of Distributed Sensor Networks, Hindawi Publishing Corporation Volume 2014, Article ID 190903, 9 pages.
9. A. Avi˘zienis, J. Laprie, B. Randell, and C. Landwehr, “Basic concepts and taxonomy of dependable and secure computing,” IEEE Transactions on Dependable and Secure Computing, vol. 1,no. 1, pp. 11–33, 2004..
10. Khaled Salah, Jose M. Alcaraz Calero, Sherali Zeadally, Sameera Al-Mulla and Mohammed Alzaabi, “Using Cloud Computing to Implement a Security Overlay Network”, IEEE Security & Privacy – 2013.
11. Lan Zhou, Vijay Varadharajan, and Michael Hitchens, “Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage”, IEEE Transactions on Information Forensics and Security, Vol. 8, No. 12, 2013.
12. Edward G. Amoroso, “Practical Methods for Securing the Cloud”, IEEE Cloud Computing 2014.
13. Eduardo B. Fernandez,Raul Monge,Keiko Hashizume, “Building a security reference architecture for cloud systems”, Springer, 2015.
14. Mazhar Ali, Samee U. Khan a, Athanasios V. Vasilakos, “Security in cloud computing: Opportunities and challenges”, Information Sciences, ELSEVIER 2015 vol 305, 357–383.
15. Chirag Modi, Dhiren Patel, Bhavesh Borisaniya, Avi Patel, Muttukrishnan Rajarajan, “A survey on security issues and solutions at different layers of Cloud computing”, Springer, 2012, 561–592.
16. Issa M. Khalil, Abdallah Khreishah and Muhammad Azeem, “Cloud Computing Security: A Survey”, Computers 2014.
17. M. Azua Himmel, F. Grossman, “Security on distributed systems: Cloud security versus traditional IT”, IBM J. RES. & DEV. VOL. 58 NO. 1 PAPER 3 January/February 2014.
18. Nelson Gonzalez, Charles Miers, Fernando Redıgolo1, Marcos Simplıcio1, Tereza Carvalho, Mats Naslund and Makan Pourzandi, “A quantitative analysis of current security concerns and solutions for cloud computing”, Springer, Journal of Cloud Computing: Advances, Systems and Applications 2012, 1:11.
19. Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez, “An analysis of security issues for cloud computing”, Journal of Internet Services and Applications 2013, 4:5
20. Hsin-Yi Tsai, Melanie Siebenhaar and André Miede, Yu-Lun Huang, Ralf Steinmetz,“Threat as a Service? Virtualization’s Impact on Cloud Security”, IT Pro Published by the IEEE Comuter Society 1520-9202 2012 IEEE
21. Xuexiu Chen, Chi Chen, Yuan Tao, Jiankun Hu, “A cloud security assessment system based on classifying and grading”, IEEE cloud computing, 2015, 2325-6095.

22. Dana petcu and Athanasios V. Vasilakos, "Portability In Clouds: Approaches And Research Opportunities", Scalable Computing: Practice and Experience 2014, Volume 15, Number 3, pp. 251–270.
23. Ashish Singh, Kakali Chatterjee, "Cloud security issues and challenges: A survey", Journal of Network and Computer Applications, Elsevier Ltd 79 (2017) 88–115.
24. Minhaj Ahmad Khan, "A survey of security issues for cloud computing", Journal of Network and Computer Applications, Elsevier Ltd 71(2016)11–29.
25. Fahad F. Alruwaili, T. Aaron Gulliver, "Secure migration to compliant cloud services: A case study", Journal of Information Security and Applications 38 (2018) 50–64.
26. Amir Taherkordi, Feroz Zahid, Yiannis Verginadis and Geir Horn, "Future Cloud Systems Design: Challenges and Research Directions", IEEE Access, Volume 6, 2018, 74120 – 74150.
27. L. Malina, J. Hajny, P. Dzurenda and V. Zeman, "Privacy-preserving security solution for cloud services", Journal of Applied Research and Technology, Vol.13, February 2015.
28. Moussa Ouedraogo, Severine Mignon, Herve Cholez, Steven Furnell and Eric Dubois, "Security transparency: the next frontier for security research in the cloud", A Springer open journal, Journal of Cloud Computing: Advances, Systems and Applications (2015) 4:12.
29. Jungwoo Ryoo, Syed Rizvi, William Aiken, and John Kissell, "Cloud Security Auditing: Challenges and Emerging Approaches", IEEE Computer and Reliability Societies, 2014, 1540-7993.
30. Kristian Beckers, Isabelle Cote, Stephan Faßbender, Maritta Heisel, Stefan Hofbauer, "A pattern-based method for establishing a cloud-specific information security management system", Req. Engineering for security, privacy & services in cloud environments, Springer-Verlag London 2013, 18:343–395.
31. Antonios Gouglidis, Ioannis Mavridis, Vincent C. Hu," Security policy verification for multi-domains in cloud systems", Springer, International Journal of Information Security (2014) 13:97–111.
32. Iram Ahmad and Archana Khandekar, "Homomorphic Encryption Method Applied to Cloud Computing", International Journal of Information & Computation Technology, ISSN 0974-2239 Volume 4, Number 15 (2014), pp. 1519-1530.
33. Vipul Goyal, Abhishek Jain, Omkant Pandey and Amit Sahai, "Bounded Ciphertext Policy Attribute Based Encryption", Springer-Verlag Berlin Heidelberg, ICALP 2008, Part II, LNCS 5126, pp. 579–591,2008.