International Journal of Computing and Mathematics
Vol. 1, Issue. 1, March 2024, pp. 7~15

Cloud Computing Cryptographic Data Security System in Banking Sector

Lim Jia Zheng[1], Aaron Frederick Bulagang[2]
[1,2]Universiti Malaysia Sabah, Malaysia

Article Info

Article history:

Received Jan 9, 2024
Revised Feb 20, 2024
Accepted Mar 11, 2024

Keywords:

IDA (Information Dispersal algorithm)
Argon2
AES (Advanced Encryption Standard)
Data Security
PBKDF2

ABSTRACT

Cloud Computing architecture and framework has gotten an acknowledgment from partnerships also, governments over the globe. Distributed computing served to decrease the cost of the executives of physical and specialized framework simultaneously has made data frameworks accessible for locally and universally conveyed work power. Cloud registering foundation gives admittance to information and applications from any area and this has made associations to continue assessing protection and security system. Banking furthermore, money related administrations have information and applications which are inside created to stay in front of rivalry. Banks need to set up another client driven condition with advancement in plans of action. Being a most inclining innovation, numerous associations need to receive mists as a practical technique, to give creative customer administrations and to increment and oversee IT productivity. In any case, banking industry despite everything has a few issues, for example, security, protection, consistence and genuineness which some place delivers an obstruction to embrace this adaptable and light-footed innovation. Efficiency, a more notable connection of all the safety aspects of the existing framework, and a straightforward and accessible solution for the customer are all provided by the new framework. In this paper, different parts of cloud figuring identified with information protection and framework security for banking and budgetary administration's industry have been presented.

Corresponding Author:

Lim Jia Zheng,
Universiti Malaysia Sabah, Malaysia.

1. INTRODUCTION

The term Cloud computing, the word 'cloud' is the analogy for the web. The term 'cloud' is inferred from the old image of cloud frequently use to speak to web in stream diagrams [1]. Through distributed computing, data frameworks assets that incorporate application, information, arrange, capacity gadgets and workers are made open what's more, accessible for use. Cloud computing essentially strikes putting away and overseeing information on virtualized workers with the goal that the client and association can get to the information everywhere throughout the world from any place at whenever. However, banks can't bear the cost of the danger of security penetrate since security of individual and money related information is the highest need for banks. Therefore, it is essential that safety factors be considered first in order to transition banks to the collaborative computing environment. The following are some benefits of adopting cloud computing in the financial industry: Reduce expenses: The banking industry's adoption of cloud computing resulted in a useful method. Even though a bank uses computer systems that are distributed, the company has nothing compelling to invest a significant amount of money in new hardware and software [1].

Furthermore, as we now know, QE uses a pay-per-use model in the cloud, enabling us to only pay for the resources that are actually needed. Enhances versatility and adaptability: The banking sector can respond to customer interests thanks to cloud computing [3]. Depending on how the business sector is developing, development can be pushed up or down.

Depending on how the business sector is developing, development can be pushed up or down. Distributed computing gives a serious extent of information reinforcement and recuperation.

Improves customer relationship: Having boundless registering powers, the cloud manufacture solid relationship with clients. Exchange banking empowers purchasers and venders share an equivalent stage with the goal that the installation procedure turns out to be increasingly proficient. [3] Nevertheless, a bank encounters many challenges when it enters cloud status. Security: Banks store their data on the cloud, raising concerns about the safety of both personal and corporate data. Banks cannot allow security threats to infiltrate [4].

Information isolation: As we realize that information on mists is put away comprehensively scattered condition so there are numerous odds for information misfortune which cause a snag [6] to receive this flourishing innovation.

Information area: When clients use cloud innovation, they have no clue about information area [6]. Scattered areas of information lead to the absence of control of information and it is exceptionally unsafe for clients.

Administrative Compliance: Customers are fundamentally at risk for the security of their information in any event, when customary specialist co-ops generally lean towards outside reviews and security authentications [5]. Information about shred workers should not be combined with other information, according to certain consistency courses of action.

Trust: Humans and machines, as well as humans and machines, should have faith in one another [7]. In the unlikely event that a client stores his sensitive data on the cloud, it is only out of trust.

Information Recovery: It implies the way toward accomplishing the information that has been lost, ruined or mishap [6].

Security and Confidentiality of information: It alludes to the attribute that information isn't available to the unapproved client [7]. As it were just approved client can get to the information and utilize any delicate information and can remove any data from that information.

Credibility of information: It suggests that there is no hardening or alteration of our data in the cloud [7].

Banking and financial administrations, industry legitimately work for the economy, thus stays matter of public significance and for the business of individuals [19]. Various security measures, such as computerized device authentication, once secret key tokens, program assurance techniques, exchange monitoring, and frameworks to detect extortion and illegal tax evasion, are implemented as part of the bank's specialized foundation [20]. These devices and systems provide banks with strong security measures while also satisfying the administrative requirements to protect customer data. As the internet grew, partnerships in banking and budgeting services started providing their products and services online and through automated teller machines (ATMs) located in remote locations, eliminating the need for customers to visit their branches. This web based financial administrations offers adaptability and accommodation in admittance to banking administrations [26]. Banks and money related administrations offer assortment of monetary items and administrations to its retail and corporate clients that incorporate web banking administrations, portable financial office, ATM withdrawals and stores, Credit card offices, Debit card offices, EFTPOS terminals, account upkeep administrations, financial exchange and depository items and forex administration. These administrations can be profited without visiting the genuine part of the bank.

2. CENTRAL THE CALCULATION FUNCTION VS. CLASSICAL HASHING

When banks are concerned about security, the secret key is the most important and crucial factor. Passwords are for the most part used to secure mystery information as in banks. The secret key plan is utilized for verification. So along these lines we can say that secret key ought to be as solid as it can make a solid divider against different gatecrashers assault like savage power assault and word reference assaults [8].

At the point when client picks a secret phrase they keep that basic and simple to retain which can be reviewed at the hour of login and furthermore some of the time clients utilize the same secret phrase for different administrations like banking, web based shopping and long range interpersonal communication sites [8]. In keeping with this, the client provides a way for programmers to access their information. The client's chosen secret phrase cannot be used as a legal cryptographic key due to its low volatility and haphazardness [9]. Therefore, a strong element is needed here to confirm the secret phrase, which in turn stimulates to confirm the cloud state.

A key determination work is probably the best answer for secure the secret key. In key induction work client picked secret word is utilized as a contribution to create at least one cryptographic key. Protecting and decoding these key cryptography is how they are used [10].

The privileged insights generated by clients with poor unpredictability and inconsistency [9] are vulnerable to attacks. Assailants discover the true identities and gain access to the records by employing thorough inquiry techniques. In line with this, graphical passwords offer 4-5 characters of protection overall and have poor entropy. They are also not complete proof plans against intrusions.

At that point a procedure called "Key extending" [8] gives protection from such assaults. Large amounts of data are processed by cryptographic hash capabilities, which then generate a fixed output known as a hash. Two messages cannot have the same hash value, and one cannot obtain a distinctive message with this value for a hash [8]. Regularly client picks a few passwords and they are put away in a database then it goes about as a secret word. Be that as it may, there is an issue as well. On the off chance that numerous clients are having a similar secret word, the hash result will be same as well. What's more, on the off chance that one of these secret words is uncovered, at that point different clients will likewise misfortune their qualifications. Similarly, if a client uses the same secret phrase for multiple services, such as banking or person-to-person communication, the security of other services may be called into question if one of these records is made public.

As a result, we have the "salt" border approach. Salt, which mostly consists of eight irregular bytes, is a little worth. An random salt is generated when a client creates a new record, and it is appended to the passwords before hashing [8]. This prevents the problem of simple hashed secret words formed by the same password. A comparable secret key generates different hashes for different records. throughout the confirmation phase, the secret phrase and salt are completed throughout the login process. The outcome is compared, and the secret key and associated hashes are stored as a means of approving [10] the client.

3. REVIEW OF LITERATURE

[3] A computation to provide data safeguarding and safety in distributed storage was proposed. They discussed cloud security, paradigms, and the cloud itself. They also suggested a data encryption computation that included a transit amount and replacement code. However, this approach was not immune to attacks by animal power.

[4] Clarified the distributed computing in banking administrations. They suggested sending the cloud banking model. They also pointed out both the positive and negative aspects of using mists in banks.

[11] Expressed that the cloud contains numerous workers and it follows customer worker design. In order to secure the cloud, he suggested a technique that combined two computations, such as the Data Encryption Standard (DES) and Computerized Signature Algorithm (DSA), with staganography to increase security. In any event, its appropriate complex nature was seen.

The level in the environment was high. Levent Ertaul [8] made the PBKDF2 and Bcrypt Scrypt computations presenting a reality. It is assumed in this study that PBKDF2 is used in many applications and was considered the most effective secret word chief. Though Bcrypt and Scrypt, or Secure are both memory-hard capabilities that require significant resources and processing power to split, PBKdF2 is fast.

This paper indicated the secret phrase hashing plan in their examination. They shed light on various problems with the current plans. They provided a memory device with hard capacity design known as Argon2. For the better uses, they recommended the Argon2. They discussed Argon2's placing orders operation, and inputs. In addition, they exemplified Argon2's strengths, such as superiority, paralleling, framework, levelheadedness, and flexibility, among others [12].

[13] One of the blum-ghetto-shub pseudo-irregular generator applications used secret key-based key induction operations. They suggested calculating a key used for encryption from a simple secret key that is difficult to remember, which sometimes makes word reference attacks and savage power attacks difficult to execute.

The work in this paper [14] proposed an upgrade for information migration in the cloud. To confirm the results, they used the sophisticated encryption standard (AES) - 256, access to knowledge Dispersion calculation (IDA), and the Secure Hashing calculation (SHA-512). For medium edges, this blend provided a guaranteed and fast execution time.

[15] Metadata cutting in multi-distributed storage was demonstrated to provide cloud security. They presented a framework for the management of multi-distributed memory. However, this method was unable to address non-revocation and other security problems.

For database in the cloud security, the paper [16] suggested crossover encryption using RSA, 3DES, and a Randon Number Generator. However, because of its staggered cryptography and decoding, this strategy adds overhead to the question execution, and its computation time increases as the size of the data increases.

4. SUGGESTED OPERATIONAL SYSTEM

Associations and banks alike must now typically store their data in dispersed storage. In any event, there are some obvious concerns that cannot be disregarded, such as security and customer protection. Therefore, this proposed work's main goal is to make certain about the protection of the financial sector, allowing banks to firmly adopt this clever invention.

The proposed work involves 3 fundamental advances:

I. Key age using a combination of Argon2 and PBKDF2

II. Using IDA (information dispersal algorithm) and AES-256 (Advanced Encryption Standard) for encryption and information slicing

III. Using IDA and the inverse of AES computation for data assembly and decoding.

IV. The suggested work's square outline looks like this:

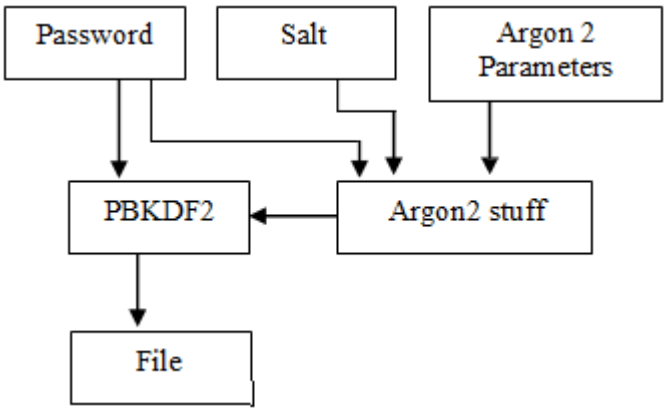

Figure 1. Proposed Working System

Secret word Based Key Derivation Function2 (PBKDF2):

The National Institute of Standards and Technology (NIST) recommends using PBKDF2 to derive the key.A technique known as PBKDF2 is used to generate cryptographic keys of a certain length from a secret key that is easy to remember or has mystery value [8]. This key is used to make advanced markings as well as to guarantee or recover the details, indicate and verify the information.

PRF is a pseudorandom capacity used by PBKDF2. HMAC typically makes these a reality. It uses SHA-256/512 as a hash computation [17]. The accompanying boundaries are accepted as input by PBKDF2:

- A random salt (s),
- a user-selected password (p),
- and the number of iterations (c)
- The length of the secret key (s_key length)

The hidden key secret_key is generated in the manner described below:

PBKDF2 (PRF, p, s, c, s_key len) = s_key

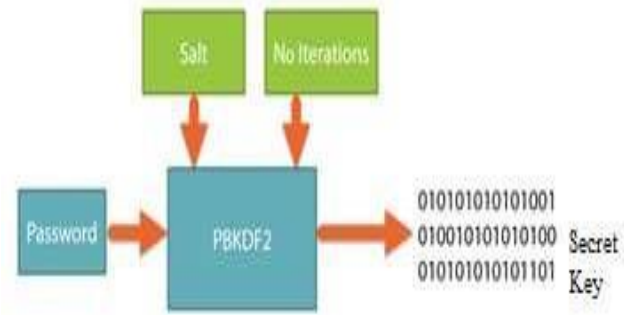

Figure 2. PBKDF2 Working

In order to produce a determined key that can be used for activities like encryption and decoding, PBKDF2 applies pseudorandom capabilities to the information secret word together with a salt value and repeats the process normally [9]. By delivering the additional computational labor (key stretching), the method of word splitting becomes more and more problematic. By incorporating saltwater to the secret word, pre-computed hashes are less vulnerable. More adjustments result in a more difficult attack. Check cycles were 1000 according to the 2000 standard, but typical programming now uses rarely over 5000 rounds [18].

The fundamental point of word reference assaults is to obtain entrance by attempting natural passwords which are put away in unique rewarded word references. There are likewise odds of savage power assaults in which assailants attempt all blend off characters [8].

The fundamental thought of utilizing PBKDF2 is that it hinders the word reference assaults and savage power assaults by expanding the time required for each endeavor of the assailant to locate the right password [9]. However, the use of salt value actually makes it possible to pre-calculate hash values and carry out table attacks.

Algorithm: The key derivation function accepts the following input parameters:

d_key= PBKDF2 (PRF, p, s, c, s_keylen) Where PRF is a pseudorandom function,
p is the user generated password from which key is generated
d is a cryptographic salt
e is the no. of counts/iterations to hash the password
d_key is the derived cryptographic key d_keylen is the desired length of secret key
Each block B_i of secret key d_key is computed as
follows: s-key =B_1‖ B_2‖ …….‖ $B_{s\_keylen/hlen}$
The Xor (^) of c, which iterates through iterated PRFs, is the function f.F (p, d, c) =Y_1^Y_2^……. ^Y_C
Where:
Y_1=PRF(p,s||INT_32_BE) Y_2=PRF (p, Y1)
Yc=PRF (p, Yc-1)

In keeping with this, PBKDF2 encourages intruders to figure out the initial secret key.

Argon2: According to PHC (2015), Argon2 is the winner of the password hashing competition. Argon2d and Argon2i are the two variants of Argon 2 [12]. Argon2d is designed to withstand attacks by animals and is dependent on information-subordinate memory access.Argon2i is primarily used for secret phrase hashing and secret key-based key determination capabilities, and it is dependent on information free memory access [18]. Argon2i is slower because it has more passes. Principal sources of knowledge and secondar98 to y entries are the two types of contributions we have to Argon2.

Essential inputs include salt(s) from (8 to 232-1) and a secret phrase (p) of length (0 to 232-1 bytes).[12] Level of complexity p, labels length, database size, number of tallies, and associated data X are examples of optional inputs. Argon2 uses BlaMka for the pressure work and Blake2b for the hash capacity.

It initially accepts inputs that are hashed along various boundaries, including the encrypted phrase (p) and salt(s). In the above, memory is addressed by [12] and is composed as a 2-d presentation. The ordering capacity is used as information for pressure work that takes place in the memory. Indexing is confidential phrase and sodium chloride free for variation Argon2i and secret phrase subordinate for variation 2d. Additionally, there is a crossover variety known as Argin2di. It is a combination of the Argon2d and Argon2i approaches. Information autonomous capabilities carry out part of the ordering in this, while information subordinate capacities handle the other component. Following the last emphasis, the recalled component of the final segment is XORed. This process repeats for a variable number of passes. It is hashed to obtain the final outcome [18].

The information dissemination algorithm, or IDA

An IDA is a method for chopping up documents and information packets so that they are unidentifiable when they are stored in dispersed areas in an organized manner [14] [15]. This clip at the accepting end, information can be reassembled with the appropriate key.

The documentation F of length L is divided into m parts Fi in this calculation, which was first proposed by Rabin [19]. The idea is that knowledge on any n pieces will aid in reconstructing the document F.

5. EXPERIMENTAL PROCEDURE

Our suggested method includes a secret phrase-based key age that uses a combination of PBKDF2 and Argon2 to generate the most secure key, adversary data encryption and decoding using AES-256

(Advanced Encryption Standard), and information dispersal calculation (IDA) to divide the data into various dispersed locations. The following are the steps for the specified methodology:

Step 1: Creation of Keys

This progression combines two estimations, such as Argon2 and PBKDF2. Salt and the client-created secret phrase will be recognized for their contributions to the PBKDF2. A mystery secret is going to be generated following the application of the necessary number of cycles and the characterization of the key's length. For the following phase of this evolution, this mystery key will serve as a secret key. Salt and the secret key—which was created in the first stage—are the two information sources that Argon2 uses in this step. Currently, there are a few preset rounds of Argon2, and a most certain key, C_key, will be generated and used as a secret key that is throughout the encryption stage.

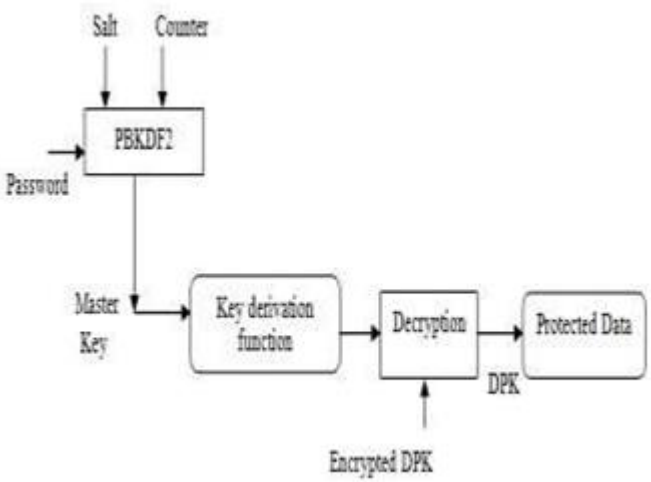

Figure 3. Creation of keys

Step 2: Data cutting and encryption

There are two security stages in this progression: information cutting using IDA computation and encryption using AES-256.

The client's unique information, or record E, is immediately jumbled using the AES-256 computation during this process. Here, the cryptographic key c_key generated in the first stage will be used. Following encryption, the jumbled document E' is divided into m separate records located in various locations. These records are spread across many locations, thus if a client is aware of at least n of these m cuts, they are typically used to put the jumbled document E'=ç(E,c_key) back together.

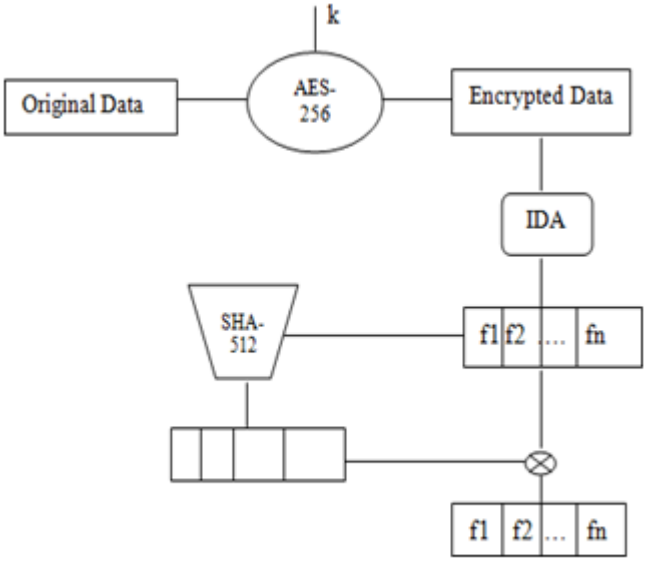

Figure 4. Steps for data chopping and encryption

Step 3: Decryption and reassembling:

The generated slices will be subjected to the IDA method in this stage, as illustrated in figure:

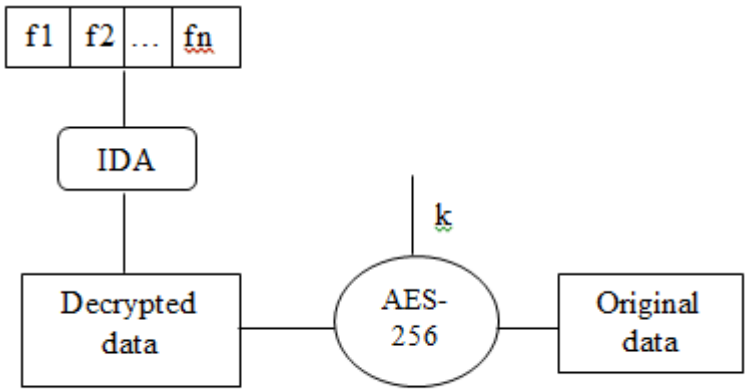

Figure 5. Reassembling and Decryption

After reassembling the encrypted file E using the IDA algorithm, we utilize AES-256 for reconstructing the original file E using the cryptographic key c key. Next, use AES-256 to calculate the decoded version of E as an E = Δ(E',c key).

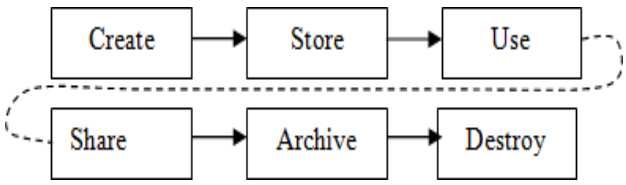

Figure 6. Lifecycle of cryptographic data security

6. FINAL RESULTS AND FUTURE DIRECTIONS

A few drawbacks of the current computations are eliminated in the suggested calculation. As we realize that the information on cloud is as a multi inhabitant condition where information and assets are shared. Therefore, it should be assured to reveal the information is verified or not in order to benefit from cloud innovation in the banking sector. We included a combination of PBKDF2, Argon2, AES-256, and IDA computation in our suggested framework. The key induction work used for key age that provides check and verification is PBKDF2 and Argon2. IDA is used to decipher the jumbled data, and AES-256 is used for information privacy. While argon2 eliminates all of pbkdf2's flaws and makes secret word hacking nearly impossible, PBKDF2 assists clients in reducing attacks. As made sure about secret word lead the made sure about the information so our methodology made sure about the secret key. Our proposition accomplishes further extent of security and furthermore better execution.

REFERENCES

[1] Abhishek Mahalle Jianming Yong Xiaohui Tao Jun Shen, "Data Privacy and System Security for Banking and Financial Services Industry based on Cloud Computing Infrastructure", (2018). Faculty of Engineering and Information Sciences - Papers: Part B. 1357.

[2] Stud. Ranjana Singh, AS. Prof Kirti Patil, AS. Prof Ashish Tiwari, "A survey on online banking authentication and data security", International Journal of Advanced Research in computer Engineering and Technology, Volume 5, Issue 2, 2016.

[3] Manisha R. shinde & Rahul D. Taur," Encryption Algorithm for data security and privacy in cloud storage", American Journal of Computer Science and Engineering Survey, Original article, ISSN 2349-7238.

[4] Dr. Sheel Ghule, Rupali Chikhale, kalpesh Kumar," Cloud Computing in Banking Services", International Journal of Scientific & Research Publications, Volume 4, Issue 6 ISSN 2250-3153, 2014.

[5] P.S.V. Sainadh, U. Satish Kumar, S. Haritha Reddy, "security issues in Cloud Computing", International Journal of Modern Trends in Science and Technology", Volume 3,special issue no.:01, ISSN: 2455-3778, 2017.

[6] Dinesh Taneja, SS Tyagi, "Information Security in Cloud Computing: A systematic Literature review and Analysis", International Journal of Scientific Engineering and Technology", Volume 6, Issue 1, ISSN: 2277-1581, 2017.

[7] Chitrali Agre," Implementation of Cloud in Banking sector", International Journal of Computer science and Information Technology research, Volume 3, Issue 2, ISSN: 2348-1196, 2015.

[8] Akshat Ajabrao Uike, Dr. M.A.Pund, "An Overview of Cloud Computing: Platforms, security Issues and Applications", International Journal of Science Technology Management and research", Volume 2, Issue 5, ISSN: 2456-0006, 2017.

[9] Levent Ertaul, Manpreet Kaur,Venkata arun Kumar R Gudise, "Implementation and performance analysis of PBKDF2, Bcrypt, Scrypt Algorithms", International conference Wireless Networks, ISSBN : 1-60132-440-5.

[10] Ackermann et. al. / "Perceived IT Security Risk of Cloud Computing, 33rd, p.3, International Conference on Information Systems, 2012

[11] Foley, John. "Private Clouds Take Shape". InformationWeek. Retrieved 2010-08-22, p2- p14

[12] Rouse, Margaret. "What is public cloud?" Definition from Whatis.com. Retrieved 12 October 2014, p1-p13.

[13] "Kevin Kelly: A Cloudbook for the Cloud". Kk.org. Retrieved 2010-08-22. http://kk.org/thetechnium/acloudbook-for/ "Vint Cerf: Despite Its Age, The Internet is Still Filled with Problems". Readwriteweb.com. Retrieved 2010-08-22.

[14] Andrea Visconti, Simone Bossi, Hany Ragab, Alexandro Calo, "On the weaknesses of PBKDF2", International Conference on Cryptography and Network security", Springer International Publishing, LNCS 9476.

[15] George Hatzivasilis," Password –Hashing Status", Journal Cryptography 1020010.

[16] Saini, Garima, Naveen Sharma, "Triple Security of Data in Cloud Computing", International Journal of Computer Sience & Information Technologies, 5.4,2014

[17] Alex Biryokov, Daniel Dinu, Dmitry Khovratovich," Argon2: the memory hard function for password hashing and other applications," version 1.3 of Argon2:PHC release, 2017.

[18] Y. D. Vybornova, "Password –based key devivation function as one of Blum-Blum- Shub Pseudo-random generator applications", 3rd International Conference," Information Technology and nanotechnology, published by Elsevier, ITNT 2017,ISSN: 1877-7058

[19] Jean Raphael Ngnie Sighom, Pin Zhang and Lin you, "Security Enhancement for Data Migration in the cloud", Future internet, 2017.

[20] Dr. K. Subramanian, F.Leo.john, "Dynamic Data Slicing in Multi Cloud Storage using Cryptographic Technique", World congress on computing and communication Technologies, 978-1-5090- 5573/17/IEEE

[21] Amanjot Kaur, Manisha Bhardwaj, "Hybrid Encryption For Cloud Database Security", International Journal of engineering Science and Advanced Technology", Volume 2, Issue 3, ISSN : 2250-3676,2012.

[22] VPN Tracker, Company Connect," Connection Safe security Architecture," equinox

[23] Turan, MS,E.Barker, W.E.Burr and L.Chen," Recommendation for password based key Derivation",http://csrc.nist.gov/publications/nis tpubs/800-132/nist- sp800-132.pdf

[24] Rabin, M.O. Efficient dispersal of Information for security, Load balancing and fault tolerance J. ACM,1989,36,335-348

[25] Dr. K. Sailaja, Prof. M. Usharani, "Cloud Computing Security Issues, Challenges and its Solutions in Financial Sectors", International Journal of Advanced Scientific Technologies, Engineering and Management Sciences (IJASTEMS-ISSN: 2454-356X) Volume.3, Special Issue.1, March.2017
[26] Aderemi A. Atayero, Oluwaseyi Feyisetan, "Security issues in cloud computing: the potentials of homomorphic encryption", Journal of Emerging Trends in Computing and Information Sciences, 2(10), 2011.