JOURNAL OF ADVANCEMENT IN ENGINEERING AND TECHNOLOGY
Journal homepage: www.scienceq.org/JAET.php
ISSN: 2348-2931 V4I3.02
Research Article Open Access

Secure Online Cloud Data Storage System Using Blowfish Algorithm

N.Jayapandian[1] and A.M.J.Md. Zubair Rahman[2]
[1]Department of Computer Science & Engg, Knowledge Institute of Technology, Salem, India.
[2]Department of Computer Science & Engg, Al-Ameen Engineering College, Erode, India.
*Corresponding author: N.Jayapandian, Phone: +91472 2433943, E-mail: njayapandian@gmail.com
Received: December 15, 2016, Accepted: February 2, 2017, Published: February 2, 2017.

ABSTRACT
The Government set aside several relief schemes for people, who are affecting in natural disasters like earthquakes, floods, cyclones and so on. The relief funds aided for the people those who are suffering in disaster. Initially, this endowment is helpful for surfers to get their basic necessary services. The benefits of this fund are transacted to sufferers through officers or politicians. But, these funds are not properly reached to the correct hands. Those funds are misused and corrupted by wrong persons. Because, the duplication of the government proofs like ration card, voter id, and so on are getting easily to corrupt the fund. To overcome that, we enhance some security levels for fund transaction through online using cloud computing. The three security levels of the proposed schemes are data collection, encryption and face detection. First, users must sign up or create an account in the relief fund transaction form. After that, the user should submit the details like family, bank details, documents that listed in that module. This submission is saved in cloud server, so it could be taken or seen from anywhere. Second, the submitted details are encrypted for more protection. Third, the user face must be detected using web cameras. All these levels is processed under a service level agreement (SLA); it is the contract between the cloud service provider (CSP) and the customer. The service provider must give assurance that, the above documents that the user submitted in cloud server will not be corrupted by any hackers. These three layers are called as tri-level security. The proposed design supports continued safe and efficient security measures, including uploaded proofs, encrypted data, and detect consumer face. By using our proposed system, hackers cannot get the money only the authorized person can receive the fund. So that, the rate of corruption will be low and also the funds will properly reach the sufferer people. Here we use Blowfish algorithm for encryption process, also we compare blowfish and hash chain algorithm. The proposed scheme the combination of face detection and blowfish algorithm give highest security level for cloud environments.

Keywords: *Blowfish algorithm, Hash Chain algorithm, Cloud Computing, Encryption, Data Storage.*

INTRODUCTION
Cloud computing is a computing design, where huge pools of schemes are coupled in distant or exposed networks, to provide animatedly scalable infrastructure for application, data and file storage. With the instigation of this technology, the charge of computation, application hosting, content storage and delivery is condensed suggestively [1]. Cloud computing is a hands-on method to experience through rate aids and it has the potential to convert a data center from a capital-intensive set up to a flexible assessed atmosphere. This idea is based on a major principal of "reusability of IT abilities". The difference that cloud computing associated to outdated perceptions of Grid computing, distributed computing, utility computing is to widen prospects through structural limitations[2].

(i) Types of Cloud Computing

Enterprises can select to organize requests on Public, Private and Hybrid clouds. Cloud integrators can play a dynamic portion in defining the accurate cloud track for each association. Public cloud is one of the quality cloud computing model, it presented off mixture applications from dissimilar clients on collective organization. The computing organization is pooled among any administrations. Public cloud is a pay-for-use model, so there is no unused source. For users, these types of clouds will offer the best savings of scale, are low-priced to set-up hardware, application and bandwidth charges are enclosed by the benefactor. There are some limits; however, the public cloud may not be correct for every organization. The model can limit conformation, safety, and SLA specificity, making it less-than-ideal for facilities using complex facts that can be focused to compliancy protocols [3]. Cloud service provider generally used virtualization method. The concept of virtualization is loading many virtual machines to the single physical storage [4]. The computing organization is committed to a specific group and not united with other groups. Some specialists articulates that private clouds are not actual instances of cloud computing. Private clouds are more exclusive and safer when associated to public clouds. A private cloud shares many of the features of public cloud computing with source combining, self-service, and elasticity and cost-for-use distributed in a consistent method with the further control and customization accessible from committed properties Private cloud is of two types. On-premise private clouds: It is also known as internal clouds and is held inside one's own data center. This model provides a more consistent process and security, but is restricted in features of scope and scalability. This is most suitable for submissions which need whole control and configurability of the organization and security.

Outwardly hosted private clouds: This type of private cloud is hosted externally with a cloud benefactor, where the benefactor enables a special cloud environment with full assurance of privacy [5]. This is best suited for creativities that don't prefer a public cloud due to allocation of physical properties. It is inexpensive than On-premise private clouds. Hybrid cloud is the grouping of private and public cloud models. Hybrid cloud is mainly prized for active or extremely variable capacities [6]. It is accomplished for providing on demand, superficially provisioned measure. By using a hybrid approach, corporations can preserve control of an internally accomplished private cloud while trusting on the public cloud as needed. For instance during peak phases distinct presentations, or portions of submissions can be migrated to the Public Cloud. This will also be helpful during probable outages like hurricane warnings, scheduled maintenance windows, rolling brown/blackouts.

RELATED WORK

As clients switch their submissions and facts to the cloud, it is serious for them to preserve, or rather exceed, the level of safety they had in their traditional IT atmosphere. The following steps offers a narrow sequence of steps for cloud consumers to assess and manage the security of their use of cloud facilities, with the goal of justifying risk and bringing an suitable level of support. The following steps will be discussed in detail below:

Step 1. Ensure operative governance, hazard and Acquiescence Procedures exist.
Step 2. Review business and operational processes.
Step 3. Manage people, roles and identities.
Step 4. Ensure data protection and information.
Step 5. Enforce confidentiality policies for cloud applications.
Step 6. Assess the security requirements.
Step 7. Ensure security of cloud networks and connections.
Step 8. Evaluate physical infrastructure and facilities are secure.
Step 9. Manage cloud service agreement in security terms.
Step 10.Understand the security requirements of the exit process.

(i) Cloud Encryption

Cloud encryption is a facility available by cloud storage benefactors whereby data or text, is transformed using encryption algorithms and is then located on a storage cloud. Cloud encryption is the conversion of customer's data into secret message. Encryption is nearly equal to in-house encryption with one significant alteration the cloud consumer must take time to study about the bill payer policies and measures for encryption and encryption key management. The cloud encryption abilities of the service benefactor need to match the level of sensitivity of the data being presented [11]

Because encryption consumes more processor above, many cloud providers will offer only basic encryption on a few record fields, such as passwords and account numbers. At this point, consuming the benefactor encrypt a customer's whole record can become so exclusive that it may make more sense to store the data in-house or encrypt the data before sending it to the cloud. To keep prices low, some cloud benefactors have been contributing replacements to encryption that don't need as much processing control. These methods comprise redacting or complicating data that needs to remain personal or the use of exclusive encryption algorithms shaped by the vendor.

(ii) Security Issues in Cloud

Cloud computing provides limitless infrastructure to store and execute customer facts and database. As customers don't need to own infrastructure, they are merely retrieving or hiring; they can forego investment outflow and consume funds as a service, paying in its place for what they use. Main Benefits of Cloud Computing is Minimized Investment outflow, Independent Location and Device, Improving Utilization and efficiency and Very high Scalability [8]. Security concerns are rising because both consumer facts and databases are residing in worker properties. Security tends to be a major concern in Open Scheme Architecture. Professional Safety operates using video investigation, state of the art interruption recognition systems and other electrical means. When an employee no longer has a commercial need to contact data center, his rights for admission datacenter should be instantly cancelled. All physical and electronic access to data centers by personnel should be registered and reviewed regularly. Review tools so that users can easily regulate how their data is warehoused, protected, used, and attest policy implementation. When user uses the cloud, user possibly won't know precisely where your data is hosted. Data should be stored and processed only in specific authorities as define by user. Provider should also make a prescribed obligation to obey local privacy necessities on behalf of their customers, Data-centered procedures that are produced when a user delivers personal or complex info that travels with that information throughout its lifetime to safeguard that the information is used only in agreement with the policy. Data store in database of benefactor should be redundantly store in multiple physical places. Data that is produced during running of program on cases is all customer data and therefore provider should not perform backups.

(iii) Data Security

Encryption is the process of duplicating essential data from a storage device. What happens to data stored in a cloud computing atmosphere once it has approved its user's "use by date". What data encryption performs does the cloud computing service provider suggest to implement for redundant and unassuming data storage devices as and when these devices are discharged or taken out of service [9]. Denial of Service: where servers and networks are brought down by an enormous amount of network stream of traffic and users are starved of the access to a certain Internet based service.

QoS Violation: Through congestion, postponing or reducing packets, or through source chopping.

IP Spoofing: Spoofing is the creation of TCP/IP packets using somebody else's IP address, so that the data can't be hacked.

Solution: Infrastructure will not permit an occurrence to send traffic with a source IP or MAC address other than its own.

The security encryption scheme is possible for all of the data to be fully encrypted. Blowfish algorithm is used for encryption. Encryption accidents can make data completely useless. The main problem of cloud service provides is doesn't give fine-grained access control in data owner [10]. The cloud provider should provide indication that encryption structures were intended and verified by skilled authorities. The main problem of cloud computing is security constraints that will be handled on availability, Integrity and confidentiality. Cloud computing is to create environment for sharing data inside and outside the cloud [7]. Security related to the info swapped between unlike hosts or between hosts and users. This issues relating to protect communication, authentication, and delegation. Secure statement issues include those safety concerns that rise during the communication between two objects. In modern world cloud computing very helpful to data storage, it gives to reduce operational cost and increase the resource utilization [12]. These include confidentiality and integrity issues. Confidentiality specifies that all data sent by users should be available to only "legitimate" receivers and reliability describes that all data received should only be sent/modified by "legitimate" senders.

PROPOSED ENCRYPTION ALGORITHM

Natural disaster causes a sudden disruption for the normal life of a society and causes damage to property and lives. So, the government allocating huge relief funds for people, who are affected in natural disasters. The relief funds are transacted to the sufferers through officers or politicians. By using that fund, sufferers will manage their basic needs. The main disadvantage of this existing system is corruption. Now-a-days, the fake documents of government proofs are getting easily to corrupt the fund. We can't identify whether the authorized or unauthorized person will get the amount. Because of this corruption, the

sufferers also can't get their rights properly.

Hash chain is the sequential application of a cryptographic hash function to a piece of data. Hash chain is also an effective method in computer security because it produces many one-time keys from a single key or password. For non-contradiction a hash function can be applied in sequence to more data. A cryptographic hash function h(x) to a string x. If a hash function of length gives a hash function of h(h(h(x))) and it is denoted h3(x). This is most often used for protection of password in an insecure environment. A server that authenticates may store a hash chain rather than a plaintext password. Also it prevents stealing of password in transaction or from the server. So, for online transaction both of these encryption and password protection algorithm are combine to use for effective and safer transaction. Blowfish algorithm is variable length with symmetric block cipher method. It's a 64bit key generation algorithm. In this algorithm main operation is user data encryption and key expansion process. The main work of this encryption process is 16 round feistel network in data encryption. Then process of key expansion is convert keys 448 bits into 4168 bytes in different sub keys [13]. The above principal blowfish algorithm functioning. Here we read different user data and follow this two sets after these process data stored in cloud server. Cloud computing is to resolve storage difficulties in various field like research laborites, government and private organizations. In current cloud technology is also lesser security model, its similar to gird computing [14]. The main objective of cloud service provider to fulfill the service level objective that means allocation and de-allocation in resources in cloud, also to minimizes the operational cost [15]. In latest cloud virtualization technology provide opportunity in complex problems like that Disaster Management System [16]. The government will manage large amount of disaster management data, cloud computing technology will provide this infrastructure [17].

Proposed Scheme for Blowfish Algorithm

The Government provides many relief schemes for people, who are affecting in natural disasters like earthquakes, floods, cyclones and so on. The relief funds are aid for the people those who are suffered in disaster. Initially, this endowment is helpful for sufferer to get their basic necessary services. The aids of this fund are transacted to sufferers through officers or politicians. First, user must sign up or create an account in relief fund transaction form. After that, user should submit the details like family, bank details, documents that listed in that module. This submission is saved in cloud server, so it could be taken or seen by anywhere. Second, the submitted details are encrypted for more protection. Third, the user face must be detected using web camera. All this levels are processed under service level agreement (SLA); it is the contract between the cloud service provider (CSP) and the customer. The service provider must give assurance that, the above documents that the user submitted in cloud server will not be corrupted by any hackers. These three layers are called as tri-level security. The proposed design supports continued safe and efficient security measures including uploaded proofs, encrypted data, and detect consumer face. By using our proposed system, hackers cannot get the money only the authorized person can receive the fund. So that, the rate of corruption will be low and also the funds will properly reach the sufferer people. Here we use Blowfish algorithm for encryption process, also we compare blowfish and hash chain algorithm. The proposed scheme the combination of face detection and blowfish algorithm give highest security level for cloud environment. The first level is to get the data from the user, the documents including bank, family, government proofs.

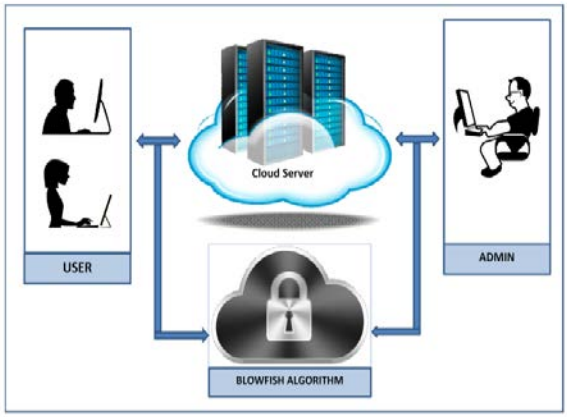

Figure 1. Proposed Tri-Level Security Architecture

The second level is to encrypt the data and documents using blowfish algorithm, that the user given in the above level. But, the decrypted data can show only to the user and the administrator. The third level is face detection, this picture will check to the documents and identify whether it is match or not. If it is matched, the fund will be transacted to the user. Else, it would be cancelled. This is the highest security system in this app to identify the correct user. The proposed system is efficient to reach the fund to sufferer and also control the corruptions. The proposed architecture is showed in Fig 1. In this experiment we collect 100 different documents and that will be stored in cloud server.

In the user registration process we use one time password security scheme. It will avoid un-authorized access to prevent user account. In the proposed scheme after user uploaded data and document immediately that documents encrypted using blowfish algorithm. It will be highly secure system even administrator is not viewed or hacked user document. Then third level security scheme we use face detection algorithm to detect exact user face identity. All these experiments we use intel core i5 server system and 8GB RAM. After collect all the test data we use Cloudsim simulator to analysis test parameters

RESULT AND DISCUSSION

In this Paper, we compare Blowfish and Hash chain algorithms. Both these algorithms are highly confidential for encrypting data, so data hacking will be very hard. A hash chain is the succeeding application for encrypting the hash function to a portion of data. In computer safety, a hash chain is a technique to produce duplication of keys from a unique key or password. For non- refusal a hash function can be applied sequentially to added sections of unique data in order to record the timeline of data's existence. Blowfish is a fast secret code, excluding when changing keys. Each new key needs pre-processor corresponding to encoding, which is very slowing associated to other block secret message. This precludes its use in definite submissions, but is not a problematic in others. In one application Blowfish's slow key altering is truly a benefit, the password-hashing method uses an algorithm derived from Blowfish that utilizes the slow key schedule; the idea is that the additional computational effort needed gives security against wordlist attacks. This limitation is not problematic though it does preclude use in the slightest implanted systems such as early smartcards. Blowfish was one of the first secure block secret message not subject to any charters and therefore easily obtainable for everyone to use. This advantage has donated to its admiration in cryptographic

software.

Encryption time analysis, we compare both algorithm to encrypt user data and documents. Compare to Hash chain algorithm blowfish taken less time to encrypt. It's shown in Fig. 2.

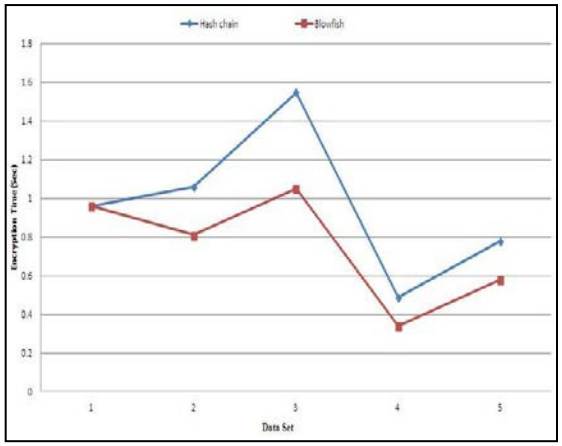

Figure 2. Encryption Time Comparison

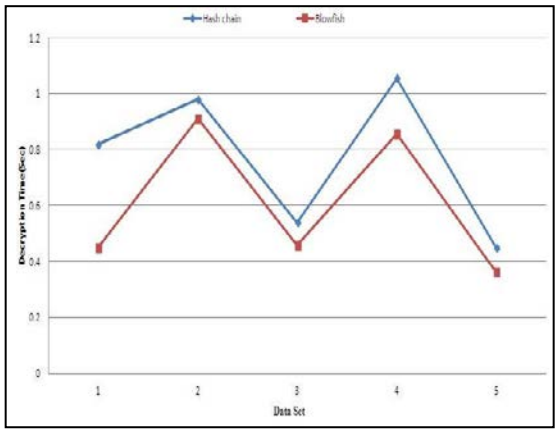

Figure 3. Decryption Time Comparison

After encryption process data stored in cloud server to verification purpose main admin to access user documents. In this process user data decrypted in same algorithm. Variation of these algorithms is 0.925%. It's shown in Fig. 3. Compare hash chain algorithm blowfish decryption very fast.

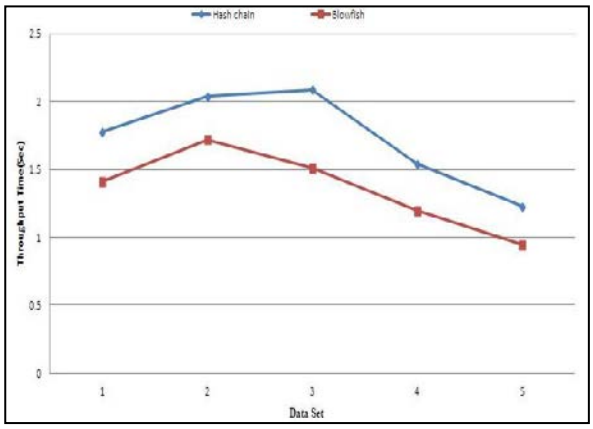

Figure 4. Throughput Time Comparison

Here throughput will be calculated overall execution time. That means the execution time of data encryption, decryption and face detection comparison. We take difference test parameter and different data sets. Fig. 4 shown in throughput time for blowfish and Hash chain algorithm. 1.86% variation for both these algorithm.

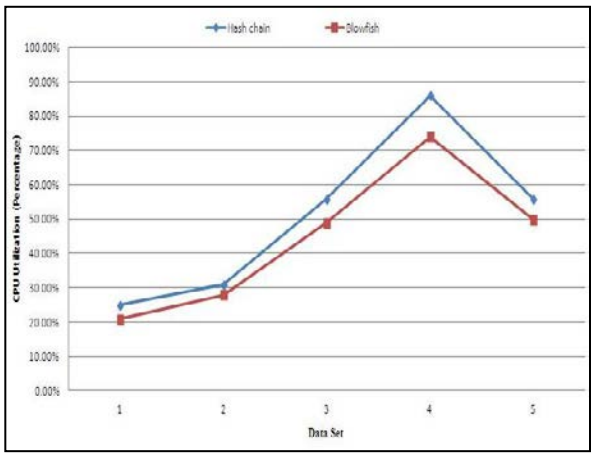

Figure 5. Throughput Time Comparison

Here we compare CPU utilization for two algorithms. CPU utilization is not much different both these algorithm execution. We take different data set some data set produce better result compare to hash chain algorithm. Fig. 5 shown in this CPU utilization percentage. Average difference for these algorithms is 8%, so it doesn't affect the system performance.

CONCLUSION

In this paper, we define and solve the problem of corruption in government disaster funds. Through this app, sufferer can get the fund without any difficulties. For that, we used some security levels for users to receiving the aid funds properly. To achieve this level, we are getting the user document for future reference. For effective process, we encrypt the user's document using blowfish algorithm. It is fast, secure, compact and symmetric block cipher algorithm. So that, the hackers can't find the user documents easily. Face detection is one of the best security methods for dodging corruption. With the comparison of this face detection and uploaded documents will show that, both are matched or not. Through analysis, we effectively create the proposed schemes for user's convenience. Our proposed schemes will definitely useful for the real-world environment and this methods dodging corruption in relief funds. Though, the aid fund will reach the sufferer hands without any double-dealing.

REFERENCES

1. R.L Grossman, "The case for cloud computing," IT professional, vol. 11, no. 2, pp. 23–27, 2009.
2. X. Xu, "From cloud computing to cloud manufacturing," Robotics and computer-integrated manufacturing, vol. 28, no. 1, pp. 75–86, Feb 2012.

3. S. Ramgovind, M.M. Eloff and E. Smith, “The management of security in cloud computing,” In 2010 Information Security for South Africa, IEEE, pp. 1–7, 2010.
4. A. Beloglazov and R. Buyya, “Energy efficient resource management in virtualized cloud data centers,” In Proceedings of the 2010 10th IEEE/ACM international conference on cluster, cloud and grid computing, IEEE Computer Society, pp. 826–831, 2010.
5. M.D. Dikaiakos, D. Katsaros, P. Mehra, G. Pallis and A. Vakali, “Cloud computing: Distributed internet computing for IT and scientific research,” IEEE Internet computing, vol. 13, no. 5, pp. 10–13, 2009.
6. N. Jayapandian, A.M.J.Md Zubair Rahman and I. Nandhini, “A novel approach for handling sensitive data with deduplication method in hybrid cloud,” In 2015 Online International Conference on Green Engineering and Technologies (IC-GET), IEEE, pp. 1–6, 2015.
7. V.P.S Kirar, “Security Architecture for Cloud Networking: A Survey,” World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering, vol. 8, no.12, pp. 2162–2165, Nov 2014.
8. S. Subashini and V. Kavitha, “A survey on security issues in service delivery models of cloud computing,” Journal of network and computer applications, vol. 34, no. 1, pp. 1–11, Jan 2011.
9. L.M Kaufman, “Data security in the world of cloud computing,” IEEE Security & Privacy, vol. 7, no. 4, pp. 61–64, Jul 2009.
10. B.P Rimal, E. Choi and I. Lumb, “A taxonomy and survey of cloud computing systems,” INC, IMS and IDC, pp. 44–51, Aug 2009.
11. N. Jayapandian, A.M.J.Md Zubair Rahman, S. Radhikadevi and M. Koushikaa, “Enhanced cloud security framework to confirm data security on asymmetric and symmetric key encryption,” IEEE World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave), pp. 1–4, Feb 2016.
12. Z. Yandong and Z. Yongsheng,“ Cloud computing and cloud security challenges,” IEEE International Symposium on Information Technology in Medicine and Education (ITME), vol. 2, pp. 1084–1088, Aug 2012.
13. O. Kara and C. Manap, “A new class of weak keys for blowfish,” In International Workshop on Fast Software Encryption, Springer Berlin Heidelberg, pp. 167–180, 2007.
14. I. Foster, Y. Zhao, I. Raicu and S. Lu, “Cloud computing and grid computing 360-degree compared,” In 2008 Grid Computing Environments Workshop, IEEE, pp. 1–10, 2008.
15. Q. Zhang, L. Cheng and R. Boutaba, “Cloud computing: state-of-the-art and research challenges,” Journal of internet services and applications, vol. 1, no. 1, pp. 7–18, May 2010.
16. D.Mendonça and W.A. Wallace, “Studying organizationally-situated improvisation in response to extreme events,” International Journal of Mass Emergencies and Disasters, vol. 22, no. 2, pp. 5–30, Aug 2004.
17. S. Kazusa, “Director for Disaster Management. Cabinet office, Government of Japan,” Published in Disaster Management of Japan, 2011.

Citation: N.Jayapandian *et al.* (2016). Secure Online Cloud Data Storage System Using Blowfish Algorithm, V4I3.02 DOI: 10.5281/zenodo.918341.