Int. J. Business Intelligence and Data Mining, Vol. 15, No. 1, 2019 49

Trust management scheme for authentication in secure cloud computing using double encryption method

P. Sathishkumar*

Department of CSE,
The Kavery Engineering College,
Mecheri, Salem, India
Email: psathishsivam@gmail.com
*Corresponding author

V. Venkatachalam

Erode Sengunthar Engineering College,
Perundurai, Erode, India
Email: profdrvv@gmail.com

Abstract: In cloud computing and banking, the consumer as well as supplier required for their service as protection and confidence. In this document suggest the belief value oriented verification procedure by the aid of encryption procedure, this verification segment bank marketing database are measured to the kernel fuzzy c-means clustering (KFCM) method. Clustered data's are accumulated in the cloud to the confidence data verification procedure. In the verification segment, the consumer verification is confirmed and acquires the verification key then encrypts the file by the double encryption algorithm. Primarily the confidence finest data implemented homomorphic encryption to encrypt the data by blowfish algorithm and then encrypted data are accumulated in cloud data core. This procedure oriented the banking data will be steadily legalised in cloud computing procedure. The outcomes are exemplify the improved encryption time and extremely legitimate the data in the cloud.

Keywords: authentication; cloud security; cloud services; trust management; clustering; cloud computing; encryption and decryption.

Reference to this paper should be made as follows: Sathishkumar, P. and Venkatachalam, V. (2019) 'Trust management scheme for authentication in secure cloud computing using double encryption method', *Int. J. Business Intelligence and Data Mining*, Vol. 15, No. 1, pp.49–70.

Biographical notes: P. Sathishkumar obtained his Bachelors degree from University of Madras Tamilnadu, India 1997, He obtained his Masters degree in Computer Applications from Bharathiar University Coimbatore, Tamilnadu, India in 2000 and Masters degree in Computer Science and Engineering from Anna University of Technology Coimbatore India in 2009, and pursuing his PhD in Computer Science and Engineering in Anna University majoring in Distributed Computing, Currently, he is an Assistant Professor in the Department of Computer Science and Engineering at The Kavery Engineering

College, Mecheri, Salem affiliated to Anna University Chennai, approved by AICTE. His research interests are distributed computing, network security and authentication, graph database, machine learning and internationalisation (i18n).

V. Venkatachalam received his BE in Electronics and Communication from Bharathiar University in 1989 and MS in Software Systems from Birla Institute of Technology in 1996. He received MTech in Computer Science from National Institute of Technology, Trichy in 2004 and the PhD from Anna University, India in 2009. From 1990 to 2000, he worked as a Lecturer at Kongu Engineering College, Perundurai, Erode. He worked as an Assistant Professor at Erode Sengunthar Engineering College from 2000 to 2008. He worked as a Principal at The Kavery Engineering College Mecheri from 2008–2016. He is currently the Principal of 'Erode Sengunthar Engineering College', Perundurai, Erode. His research interests are network security and cryptography, data mining, artificial intelligence and wireless networks. He is a life member of the Indian Society of Technical Education (ISTE).

1 Introduction

Cloud computing is a method of distributing computing applications to execute websites and web applications. E-commerce enchanting the benefit of cloud computing platform afford for distributing applications, services and details between public across the globe (Chonga et al., 2014). Based on the different appearance of the condition of services, cloud computing can be recognised as software as a service (SaaS), platform as a service (PaaS) or even infrastructure as a service (IaaS) (Li et al., 2010). This is a key method where the data is composed by several isolation and secrecy limitation requisite either by the application or by managers (Krishna et al., 2012). Cloud suppliers permit the consumer to contact details and business procedure by specific authorisation, which means an open stream of details and a confidence association linking the cloud supplier, further cloud supplier, and clients (Kretzschmar and Golling, 2011). Consequently, numerous defence representation and confidence founding method have been organised and are been in implementation for supplying extra protection to the data, particularly the responsive data (Saeed and Khan, 2015). Data security is accomplished by employing cryptographic algorithms. The exploit of public clouds necessitates confidence of businesses on cloud service supplier (Pawar et al., 2014). A classifier, which is equipped for self-sorting exposed its learning from gushing information, is profoundly coveted for adapting to certifiable information streams (Pratama et al., 2016a). Also, the classifier ought to be versatile to develop huge information streams, since substantial volumes of information are persistently created from sensors, the internet, and so on, at a high approaching rate in today's real world issues. A retraining procedure is done in customary classifiers (Pratama et al., 2015b; Lughofer and Pratama, 2017). The noteworthy obstruction is the developing non-stationary nature of learning situations, summoning classifiers endued independent from someone else adaptable restorative aptitudes for tractable operation administrations of the framework being handled (Pratama et al., 2015a). The remuneration necessitates being reasonable by the impending hazard that approaches from cloud computing. Illegal invader can openly contact to one

resource for several companies and consumer responsive data relatively than offensive several networks and consumer (Tang and Liu, 2015).

The analysis demonstrates that this strategy is both productive and viable for the kernel classifier learning. Nonetheless, the objective of kernel classification is not to learn great classifiers themselves. Due to this favourable position, another kernel-incited is the remove measure for the first information space into target capacity of FCM (KFCM) to supplant the routine measures. In the meantime, a punishment term considers the impact of neighbouring pixels on the focal pixel (Wang and Wang, 2014; Aliahmadipour et al., 2017). As of late, some fuzzy connection-based strategies are proposed to extension clustering and classification (Gong et al., 2013), which additionally has a place with the principal class. Fuzzy clustering (FRC) articulates a straightforward contrasting option to customary discovery methods, for example, neural systems. To upgrade FRC's strength by supplanting FCM and hard class marks with KFCM and delicate names, independently (Bo et al., 2014). This can start its enchanting in process sans preparation with an unfilled manage-base and naturally include, prune, blend its fluffy guidelines from information streams a short time afterwards (Pratamaa et al., 2016c).

In recent times, trust-based application choice is also concerned as major study assistance (Li et al., 2012). They interested on estimating loyalty of application, which can be considered as a broad superiority computes of application. There are primarily two processes for estimating dependability of application (Tanga et al., 2016). Away from the several applications that cloud computing recommends, population also utilise the cloud as a storage region, which can be expressed as data outsourcing. A consumer accumulates his data on the cloud thus the data can be recovered shortly (Srisakthi and Shanthi, 2015). A novel evolving type-2 recurrent fuzzy neural network (eT2RFNN), which is fit for settling each of the three hidden issues in an online mode: instability, worldly framework element, and framework arrange. ET2RFNN constitutes a completely developing and versatile learning calculation (Pratama et al., 2016b, 2014). There is a grave constraint to tackle the data protection problem for defending the data reliability, isolation and confidence in the cloud atmosphere (Sirohi and Agarwal, 2015). Elevated protection is the chief blockage for breaching the novel period of extended dreamed idea of computing as a service. Because of the responsive applications, data are stimulated into the cloud data hub and execute on practical computing possessions in the outline of the practical machine (Suna et al., 2011).

The symmetric-key and asymmetric-key algorithms can be utilised for encrypt the data at cloud storage. Cloud storage has a huge group of databases and a great database asymmetric-key algorithm's presentation is deliberated when contrast to symmetric-key algorithms (Khan and Tuteja, 2015). Generating and organising a protected cloud gap is demanding charge. Cloud data protection relies on implementing suitable data protection actions and countermeasures. Each one encryption process has individual qualities and disadvantages (Shereek et al., 2014). Trust management has been acknowledged as a very important element for launching and preserving flourishing relational connections among e-commerce operating associates in cloud atmosphere (Habib et al., 2010). The contention degree incited by the datum is examined by two govern developing cursors named a sort 2 rendition of the data quality technique and the datum significance idea, to decide a reasonable learning situation for investigating the datum (Pratamaa et al., 2016d, 2016e; Venkatesan et al., 2016). Once the datum qualifies as another fluffy control, its parameters are initialised by initiating the Bayesian class covering basis to evade a covering district, incited by another lead (Lughofer et al., 2015).

It carries clients in constantly classifying reliable cloud supplier, and to direct the confidence associations among business associates in cloud atmosphere. This is attained by preserving the trust-level of the e-commerce applicant and formulates them obtainable to impending e-commerce clients when desirable (Chonga et al., 2014). Authorised concern about cloud clarification can approach from client convention and/or from nationalised necessities on isolation and a permissible interception. Even though the concluding is specified to the telecommunication production it is essential to locate traditions to hold them over into cloud clarification (Martucci et al., 2012). In Section 2 there is an elaborate description regarding the literary reviews. Section 3 is rich with colourful data on the proposed technique. In Section 4 discuss the results of trust model clustering and encryption technique and existing technique. The section ends with a befitting conclusion.

2 Literature review

In 2016, Chiregi et al. have offered the confidence by allowing for the authority of estimation privileged on further units and eliminating the troll units achieve in the cloud atmosphere. The confidence value is estimated by five limitations such as accessibility, dependability, data integrity, uniqueness and potential. As well, suggest a technique for estimation privileged and troll unit classification by three topological measurements with input-degree, output-degree and reputation procedures. The technique is estimated in a different condition where illustrate the outcome of exactness by eliminating the outcome of troll units and the suggestion of estimation privileged.

In 2015, Bharathia et al. have recommended an extensive confidence administration format which employs a variety of quality of the cloud computing atmosphere. The confidence computing carried out by user profiles, and the key-based system does not bear the firewalls for unbeaten working and presentation progress. At this time the position detail of the consumer is utilised to evade applications from objective by the wicked consumer. It also utilises a time alternative hashing system to calculate private keys for the legal consumer. On the scale of being safe, the applications from objective attack employed an actual time service work method, which unites needed applications based on the position of the consumer and further measures.

Confidence representation for determining defence power of cloud computing service by Shaikha and Sasikumar in 2015 has recommended a quantity by using a trust model. A trust model dealings the defence power and calculate a confidence value. A confidence value encompasses of different limitations that are essential proportions beside which protection of cloud services can be deliberate. Cloud service alliance (CSA) service disputes are utilised to review protection of a service and strength of the representation. Sufficiency of the representation was also established by estimating confidence value for obtainable cloud services. Trust model performed as a standard and status service to compute protection in a cloud computing atmosphere.

In 2015, Agre cloud equipment recommend business representation for distributing original customer knowledge, effectual cooperation, improved speed to market and better IT effectiveness. By cloud computing banks can generate a bendable and responsive banking atmosphere that can rapidly take action to novel business requirements. This effort cloud computing can be employed in the banking trade, different business

representation related with it and the troubles expressed by the banking trade in approving this equipment.

In 2014, Fan and Perros have projected the difficulty of confidence management in multi-cloud atmosphere depend on a group of circulated trust service providers (TSPs). These are autonomous third-party supplier/confidence mediator, confidence by cloud providers (CPs), cloud service providers (CSPs) and cloud service users (CSUs) that provide confidence interrelated applications to cloud contributor. TSPs were circulated above the clouds, and they extract unprocessed confidence facts from dissimilar resources and in the diverse set-up. Testing illustrates that projected structure is effectual and comparatively steady in discriminating trustworthy and untrustworthy CSPs in a multi-cloud atmosphere.

In 2013, Huang and Nicol have recommended the confidence was a grave feature in cloud computing; in existing achievement relies mostly on observation of status, and personality evaluation by the supplier of cloud services. Next tackle those boundaries by suggesting more precise system depend on confirmation, characteristic guarantee, and legalisation, and terminate by signifying a structure for incorporating different trust methods collectively to expose chains of confidence in the cloud.

In 2013, Bose et al. have recommended the position of protection and confidence in cloud computing atmosphere from the view of association would delegate their confidential details to the cloud computing supplier. For some novel tools such as cloud computing confidence is not effortlessly recognised, it steadily constructed relies on supplier standing for fine presentation and protection, receiving consumer confidence over time. The customers must believe the cloud supplier like confidence banks to deposit their money into them. Likewise, the cloud supplier must reveal that they are consistent and responsible. So for extensive implementation of cloud computing, compete that clients should be capable of accumulating their data in the cloud among similar assurance as they accumulate their money and extra treasure in the banks nowadays.

In 2016, Stergioua et al. have proposed the primary objective of communication and participation amongst things and articles which sent through the wireless systems is to satisfy the target set to them as a joined substance. Also, there was a fast improvement of both innovations, cloud computing and internet of things, respect the field of wireless communications. Exhibit an overview of IoT and cloud computing with an emphasis on the security issues of both innovations. In particular, they join the two previously mentioned advancements (i.e., cloud computing and IoT) with a specific end goal to look at the basic elements, and so as to find the advantages of their coordination. Concluding, they showed the commitment of cloud computing to the IoT innovation. Subsequently, it indicates how the cloud computing innovation enhances the capacity of the IoT.

In 2016, Gupta and Badve have proposed the denial-of-service (DoS) attack and distributed denial-of-service (DDoS) attack can fundamentally trade off accessibility of the framework services and can be effortlessly begun by utilising different devices, prompting to money related harm or influencing the notoriety. The DoS attack and distributed DoS attack that can be completed in cloud environment and conceivable protective instruments, devices and gadgets. What's more, they talk about many open issues and difficulties in shielding cloud environment against DoS attack.

In 2013, Negi et al. propose a change to the certainty-based filtering strategy (CBF) which is explored for distributed computing environment in light of connection example to moderate DDoS attacks on cloud. The change presents ostensible extra bandwidth and tries to expand the handling rate of the casualty started the server.

GARCH and ANN-based DDoS detection and filtering in cloud computing environment by Gupta and Badve in 2015 had proposed strategy which can distinguish and channel different DDoS attacks in cloud environments. It utilises a nonlinear time arrangement (GARCH) model to effectively foresee the activity state as it can catch long-range dependence (LRD) and long-tail conveyance, which is the property of general network movement. In addition, bedlam hypothesis is utilised for the DDoS attack discovery. Sifting is finished with the assistance of a back-propagation artificial neural network (ANN) on the movement that surpasses as far as possibly indicated by some limit. The test comes about demonstrate the matchless quality of the proposed approach over different methodologies.

In Yamad and Ikeda (2017) have proposed a data structure to enhance public key infrastructure (PKI) authentication was proposed generalising the concept of ISO/IEC 24761. Current innovations do not give adequate information on items which are utilised as a part of the authentication procedure at claimant to the verifier. Accordingly, the verifier cannot adequately distinguish the authentication result executed with a trusted item from without a trusted item. The distinction was made clear if confirm data of the execution of authentication process at the claimant was generated by the trusted item and utilised for verification by the verifier. The data structure for such data is proposed in this paper as a customer authentication context (CAC) instance. Relation to different works and extension of the proposal where biometrics is utilised as portrayed for a further change of PKI authentication.

In Ciobanu et al. (2017) have proposed an entrepreneurial trust and reputation mechanism entitled SAROS, which distinguishes and avoids malicious hubs, i.e., hubs which, receiving messages for other interested companions; change their content so as to spread false information. This can negatively affect the system, by polluting it with spam messages or dropping messages of interest to the hubs in the system. By detecting and avoiding malicious hubs, SAROS can increase the percentage of right messages that reach their destinations.

In Singh and Sidhu (2017) have proposed a compliance-based multi-dimensional trust evaluation system (CMTES) that enables CCs to determine the trustworthiness of a CSP from alternate points of view, as trust is a subjective concept. Such a framework is of great help to CCs who want to pick a CSP from a pool of CSPs, satisfying their coveted QoS necessities. The framework enables us to evaluate the trustworthiness of a CSP from the CC's point of view, cloud auditor's viewpoint, cloud broker's point of view and peers' viewpoint. Experimental outcomes demonstrate that the CMTES is compelling and stable in differentiating trustworthy and untrustworthy CSPs. The validation of the CMTES has been done with the assistance of manufactured data because of lack of standardised dataset and its applicability has been demonstrated with the assistance of a case think about involving the utilisation of real cloud data.

Multifaceted trust management framework based on a trust level agreement in a collaborative cloud by Varalakshmi and Judgi (2016) had requested for prepared by an untrustworthy supplier can endanger the quality of administration, prompting the dissatisfaction of the client. This paper aims to choose the trustworthy service provider (TSP) by evaluating trust based on in-context feedback from various sources; these sources include client feedback, global advisory feedback, and outsider feedback. Besides, unfair feedback is shifted to enhance accuracy. Consequently, the occupation achievement rate increases and clients are able to obtain value-for-money for the entirety paid toward selection of a supplier. The present experimental work demonstrates that the

proposed model is successful and productive in selecting a trustworthy supplier in a collaborative environment.

In Kumar and Jain (2015) had planned to safely store and access of data via the internet. The brisk development in the field of 'cloud computing' has also increased data security concerns. Security is a constant issue for open frameworks and internet. When we are thinking about security, cloud really endures a ton. Lack of security is the greatest obstacle in wide adoption of cloud computing. The weakness in client's authentication procedure, integrity and lack of powerful security strategy in cloud storage leads to many challenges in cloud computing. Authors have proposed a twofold encryption conspire that not only gives security of client's private data during storage and access over the cloud they additionally gives the authentication feature using Elliptic bend cryptography.

2.1 Problem identification

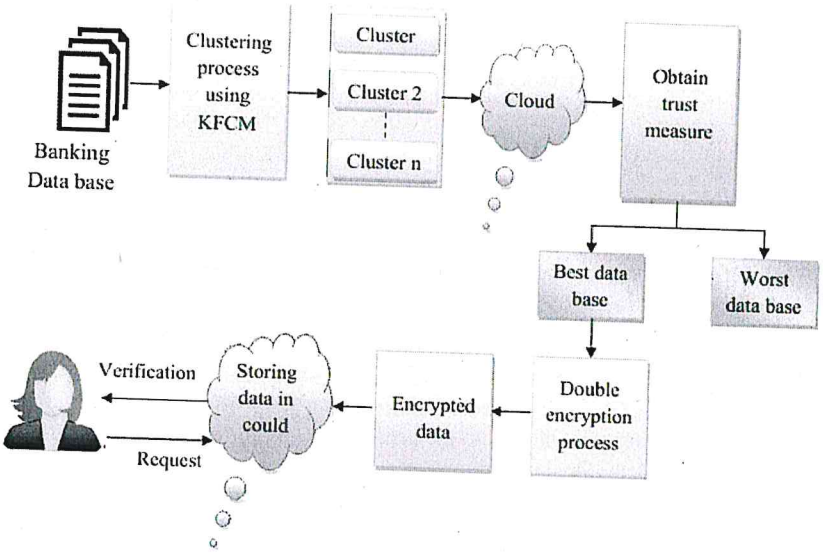
- The common problems in existing cloud security approaches are given below.
- Cloud stores do not have the capacity to oversee information provenance. Information provenance should be secured since it might uncover private data about the touchy information while the cloud specialist enclosure does not ensure secrecy of the information put away in scattered geological areas.
- Distributed storage brings a few security issues. Information secrecy shows positive as the greatest sympathy toward clients of a distributed storage framework.
- In the confidentially distributed computing condition furthermore, you will believe the cloud supplier for individual information storage.
- The principle two issues in distributed computing are the client experience when utilising distributed computing administrations. The first is clients' worries about hacking dangers whether inside or remotely. The other one is the infeasibility of encoding all information without mulling over of its classification degree.
- Existing encryption technique ECC is utilised for authentication handle, ECC strategy is validation, or encryption calculation, to the private key and open key generation practice. In outsider send the demand implies the answer messages that are encoded by introducers' mystery keys, unscrambles the messages with the comparing open keys.

3 Proposed methodology

Cloud computing is a revolutionary computing approach, which provides massive storage and computational capability. It provides user to implement applications cost effectively without investment and infrastructure. The objective of this proposed work is to develop the modelling for trust management authentication in cloud computing using double encryption method. Initially, consider the bank marketing databases to clustering process. Cluster the data using kernel fuzzy C-means (KFCM) clustering algorithm is used, after this clustering process, the data into different clusters are randomly stored in the cloud to find the trust values. This trust measure evaluation process threshold value is considered. If the trust measure is maximum compared with threshold this data are worst data's and

the measure is minimum compared with threshold the data are best-trusted data. The trust level is derived from feedback ratings submitted by the trading partners after the successful completion of the transactions. This best trusted to the authentication process using double encryption method. In each cluster best data applied the 'homomorphic encryption algorithm' is used to encrypt the data based on the private key and public key. Then the encrypted data is allowed into second encryption method blowfish algorithm is to encrypt again the data. This encrypted data are stored in the cloud to the authentication phase. In authentication phase, the user data is confirmed for the purpose of authentication and subsequently, the data is encrypted for the securing procedure. The third party auditor is allowed to access the user data, after getting the node from the user for the eventual authentication of the data and this user data in which cluster are identified. Following the above processes, the data is authenticated in the cloud. The comprehensive function of the novel technique is effectively exhibited in the block diagram appearing in Figure 1.

Figure 1 Block diagram for proposed method (see online version for colours)



3.1 Initial setup

The primary unit is consumer expose their detail and record in the cloud server. If the registration is exploiting the consumer or holder obtains their equivalent private key. If the consumer was previously recorded their details in the cloud server which means the consumer certification is confirmed. If the certification is achieved then the consumer approved to contact the cloud server or else the consumer demand is discarded. Subsequently, the projected technique employs kernel fuzzy c means clustering algorithm is to set the supply and it depends on the supply category. The comprehensible design of KFCM clustering algorithm is exemplified as underneath.

3.2 Data clustering using Kernel-based fuzzy C-means clustering

Clustering systems are the main element invalid system that can be operated to arrange detail into an assembly in the beam of resemblance between the personality data substance. Generally, clustering algorithms do not rely on supposition standard to the predictable arithmetical system. This clustering procedure-based evades detail failure and develop the presentation in verification procedure.

KFCM

The novelty of KFCM process is to cluster the data from the database with similarity measure is proposed. It reduces the quantity of key points generated and increases the number of matching key points at the same time by employing KFCM. Therefore, the matching score defined as the ratio between the number of matching key points and the number of key points generated is improved. Moreover, the computational complexity is reduced due to the reduction of information in each data by extracting brightness of data.

Fuzzy C-means (FCM) is a system of clustering which permits detail indicates to assembly in the analysis of imminence and essentially exploited in outline identification. The transform of goal task by diminishing as obtain the following:

$$O_m = \sum_{i=1}^{n}\sum_{j=1}^{c} u_{ij}^{m} \left\| x_i - c_j \right\|^2 \tag{1}$$

where m is areal number higher than 1, u_{ij}^{m} is the degree of membership, x_i is the cluster, j is the d-dimensional measured information, c_j is the d-dimension centre of the cluster. Fuzzy classification is finished by objective function iteration as appeared above, with the update of membership u_{ij}^{m} and the cluster centres.

Iteration of this procedure will be wrecked when there is conclusion stipulation where approximately 0 and 1, while k are the iteration pace and N is the entire number of clusters. This approach focalises to a local minimum or a saddle point of J_m. This KFCM procedure regarded as the input as dissimilar papers and output as clustered file depends on the dissimilar keywords.

Procedure

1 Kernel version of the FCM algorithm and its objective function are given bellow:

$$O_m = \sum_{i=1}^{n}\sum_{j=1}^{c} u_{ij}^{m} \left(1 - K\left(x_j - C_i\right)\right) \tag{2}$$

2 Compute the fuzzy centres c_j

$$C_i = \frac{\sum_{j=1}^{n} u_{ij}^{m} K\left(x_j, C_i\right) x_j}{\sum_{j=1}^{n} u_{ij}^{m} K\left(x_j, C_i\right)}; \quad i = 1, 2 \ldots C \tag{3}$$

3 Calculate the fuzzy membership function u_{ij} using

$$u_{ij} = \frac{\left(1-K\left(x_j, C_i\right)\right)^{-1/(m-1)}}{\sum_{j=1}^{n}\left(1-K\left(x_j, C_i\right)\right)^{-1/(m-1)}}; \quad i=1,2\ldots C \tag{4}$$

4 Repeat step 2 and 3 until the maximum of O_m value is achieved.

Identify the essential conditions for minimising O_m is revise equations (3) and (4) only when the kernel function K is selected to be the Gaussian function with $K(x_j, C_i) = \exp(-\|x_j - C_i\|^2/\sigma^2)$. Different kernels can be selected by replacing the Euclidean distance for different conditions. However, a Gaussian kernel is appropriate for clustering in which it can essentially make the essential conditions. The clustered data stored in cloud obtain the trust model process.

3.3 *Trust model*

The trust model analyses the values for different cloud applications. Cloud consumers desire to exploit one of the cloud applications relies upon their requests. A cloud consumer can move towards to a cloud application director for the essential applications. Trust model performs as gathering applications to resolve the safety power of the cloud applications. It estimates both the inactive and active confidence value of protection that can be employing by the consumer to resolve protection and character of cloud applications. This clustered data confidence assess renovates the entry value then discover the confidence quantify by beneath equation.

$$V_1 \sim V_2 = 1-(1-V_2)^{V_1} \tag{6}$$

where V_1 is recommendation trust value and V_2 direct trust value

The verification procedure values go between 0 and 1. By the deliberation in our system representation, classify an express confidence association as the confidence association among two nodes in the equivalent collection and a reference confidence as the confidence association among nodes in the dissimilar collection. Concern the equations for estimated and amalgamation of confidence values from the express confidence and the suggestion confidence value. These confidence data computations attach the threshold value contrast by confidence quantify. If the confidence measures away from threshold the data region expected finest data to the certification procedure.

3.4 *Authentication phase*

Authentication in our system relies on the public key credential indicated by a few trustable nodes. Each node is competent to demand public key credential of some other novel nodes. Though, nodes in the identical set are implicit to identify each other by their observing mechanism and the small objectivity with them. Subsequent to decide the confidence data the certification procedure will be utilised to encrypt the data, now initial phase homomorphic encryption method are exploited then the second phase procedure are encrypted data over again and operate to blowfish encryption method.

3.4.1 Homomorphic encryption algorithm

Homomorphic encryption structures are utilised to execute a procedure on encrypted data lacking noteworthy the private key (without decryption), the customer is the only proprietor of the secret key. The homomorphic encryption is a method that permits the calculation on encrypted data lacking preceding decryption, and following procedure if the user decrypts the outcome, which is in the encrypted outline. The compound precise procedure can be carried out on the cipher text lacking altering the character of the encryption (Ahmad and Khandekar, 2014).

Functions of homomorphic encryption

Homomorphic encryption process consists of four functions H.

$$H = \{Key\ Generation,\ Encryption,\ Decryption,\ Evaluation\}$$

Key Generation	the client will generate a pair of keys public key K_p and secret key K_S for encryption of plaintext
Encryption	using secret key K_S client encrypt the plain text T_p and generate $EK_S(T_p)$ and along with public key K_p this cipher text T_C will be sent to the server
Evaluation	Server has a function f for doing an evaluation of cipher text T_C and performed this as per the required function using K_p
Decryption	generated $Eval(f(K_p))$ will be decrypted by the client using its K_S and it gets the original result.

Pseudo code for Homomorphic encryption process

***Key generation**: KeyGen(m, n).*

Step 1: Choose two large prime numbers m and n randomly

Step 2: Compute $k = mn$ and $\alpha = lcm(p-1, q-1)$

Step 3: Select random integer value i, where $i \in Z_{k^2}$

Step 4: Random value i checking the existence $\mu = (L(i^{\alpha} \bmod k^2), k) = 1$ where $L(u) = u - 1/k$

Step 5: Public encryption key $K_p = (k, i)$ and $K_S = (m, n)$

***Encryption:** Enc(e, K_p)*

Step 6: Let i be a message to be encrypted where $e \in Z_k$

Step 7: Select random variable $r \therefore r \in Z_k^*$

Step 8: Compute cipher text $c = i^e . r^k \bmod k^2$ $r \therefore r \in Z_k^*$ $\therefore c \in Z_{k^2}$

***Decryption:** Enc(c, K_S)*

Step 9: Let c be the cipher text to decrypt where $c \in Z_{k^2}^*$

Step 10: Compute plain text $e = \dfrac{L(c^{\alpha} \bmod k^2)}{L(i^{\alpha} \bmod k^2)} \bmod k$

Homomorphic encryption is a semantically protected cryptographic scheme, in the sense that users can delegate the processing work on their private data. This encryption process-based encrypted the data in trust management process.

3.4.2 *Blowfish encryption method*

The blowfish method has been successfully and widely engaged for the principle of accomplishing the symmetric key cryptography. In the revolutionary method, the Blow Fish method is sophisticatedly engaged for both the encryption and decryption. It includes the 64-bit block dimension and key length from 32 bit to 448 bits. There is the occurrence of the P-array and four 32 bit S-boxes. The P-array involves 18 of 32-bitsubkeys and each S-box is residence to 256 entrances (Fan and Perros, 2014). The key development is delegated by the assignment of efficiently implementing the conversion of the input key (448 bit) into sub-key (4,168 bytes) arrays. The data encryption takes up the 16 round Feistel system, among each encircling endowed by a key reliant combination and a key reliant changeover. Each and every one of the task signifies those of the XOR and the embellishments on 32-bit words in the blowfish method.

Sub-keys of blowfish algorithm

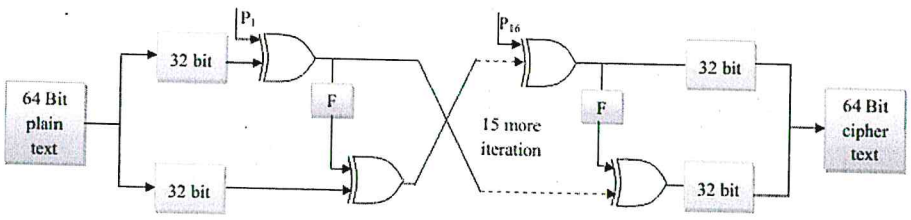
An extremely large number of sub-keys are deployed in the blowfish technique, and they have to be invariably pre-computed before carrying out the encryption and decryption processes.

- P-array consist of 18 of 32-bitsubkeys
- four 32 bit S-box contains 256 entries.

3.4.2.1 *Encryption*

The encryption signifies the assignment of renovating fundamental text into the difficult cipher text. In the epoch-making method, the input employs 64-bit data, which, is in the preliminary encircling, it is separated into two 32 bit bisect, that is marked as the left halves (LH) and right halves (RH). In the original blowfish algorithm, the primary 32 bit LH and the P-array carry out the XOR task and the result is to deliver the function (F) revealed in Figure 2. Afterward, carry out the XOR task for equally LH and the subsequently 32 bit RH gracefully. This is chase by the transaction of both the result. Subsequently, remaining of the encircling are prolonged until the accomplishment of 16 rounds.

Figure 2 Blowfish algorithm process (see online version for colours)



3.4.2.2 Process of F function

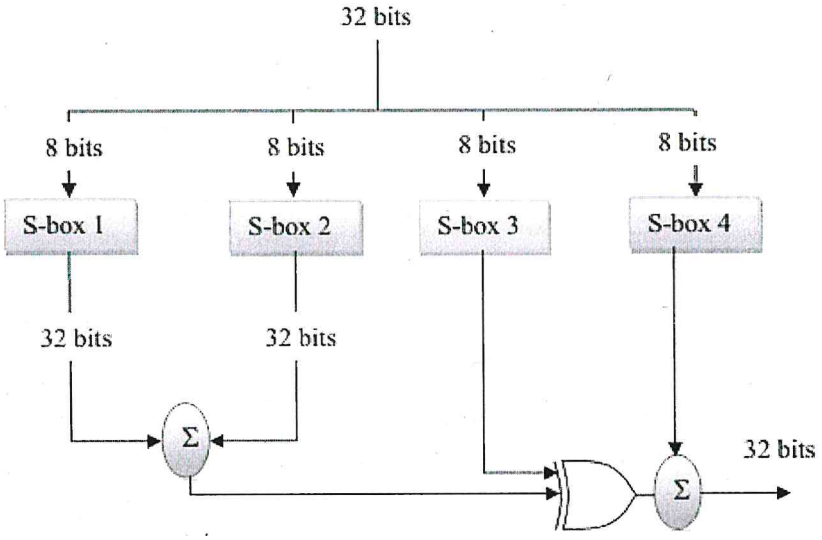
The F function deploys four 32 bit S-boxes, with each one encompassing 256 entries. In the novel blowfish technique, the initial 32 bit LH are subdivided into four 8 bit blocks such as m, n, o, and p.

The formula employing the F_t function is elegantly exhibited in the ensuing equation (1).

$$F(L_H) = \left(\left(S_{b1,m} + S_{b2,n} \bmod 2^{32}\right) \oplus S_{b3,o}\right) + S_{b4,p} \bmod 2^{32} \tag{7}$$

The detailed working process of F function is shown in Figure 3.

Figure 3 Working process of f function (see online version for colours)



3.4.2.3 Decryption

The decryption system of the blowfish method is alike to that of the encryption, even if it occurs earlier; the P-array is engaged in the repeal. The productivity of the blowfish method accumulates the folder in the cloud, which is arranged as the input of the second segment. By the support of the communal and personal keys, the folder experiences the task of encryption and acquire uploaded into the cloud.

Pseudo code for blowfish algorithm	
Step 1:	Read the 64 bit input data X
Step 2:	Input data X divided into two equal parts x_1 and x_2
Step 3:	For $i = 0$ to 15
	$x_1 = x_1$ *XOR* x_2
	$X_2 = f(x_1)$ *XOR* x_2
Step 4:	Exchange x_1 and x_2

Step 5: Again exchange x_1 and x_2 (go to step 4)
$x_1 = x_1 \; XOR \; P_{18}$
$x_1 = x_1 \; XOR \; P_{17}$
Step 6: Combine x_1 and x_2

The S-boxes and P-boxes are initiated by standards from hex digits of pi. The variable length user-input key is afterward XOR by P-entries. Subsequently, a mass of zeros is encrypted, and this outcome is utilised for P1 and P2 access. This double encryption procedure oriented to encrypt the confidence data in the cloud to the protection principle. In experiment procedure, the third party offers the demand to encrypted cloud data method the demand will be established or discarded and also the specified data in the cluster also recognised.

4 Result and discussion

This section gives the detailed view of the result that is obtained by our proposed method of secured data authentication process in the cloud. This proposed work implemented in java programming language with JDK 1.7.0 in a windows machine containing configurations Intel (R) Core i5 processor, 1.6 GHz, 4 GB RAM and the operation system platform is Microsoft Wnidow7 Professional. The experimental result and the performance of the proposed method are given below in detail.

4.1 Database description

The Java successfully classifies the memory for use. Novel objects are created and situated in the heap. When your request does not enclose several suggestions to an object, then the Java garbage collector occupy the effort of exclusion of the correlated object and eliminate it from the memory that your request is proficient in utilising the qualified memory supplementary.

4.2 Performance evaluation parameters

This section provides the performance analysis of encryption time and memory usage at different threshold values. In addition to this, it also depicts the memory usage and encryption time for various memory size.

Memory usage

The Java effectively organises the memory for use. New objects are generated and positioned in the heap. When your application does not contain any reference to an object, the Java garbage collector takes up the work of elimination of the related object and removes it from the memory in order that your application is competent to employ the relative memory further.

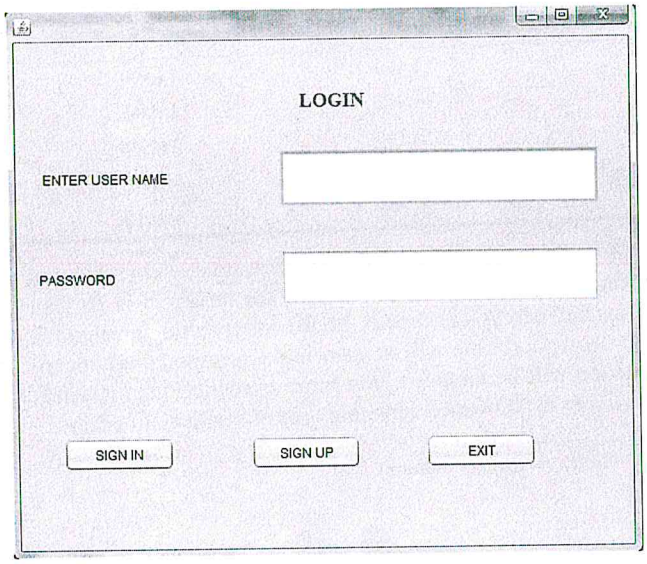
Encryption time

Time taken to recognise the algorithm in encryption and decryption procedure is encrypted time. The execution time in the Java program is squarely entrenched on depends on the remembrance and database values. The time obstacle is consistently signified in such a manner as to disregard the coefficients and minor regulate conditions and in the time period is calculated in millisecond (ms).

4.3 Experimental result

The investigational outcome of the projected system is revealed in beneath. Initially, the consumer records their particulars in the cloud server. The novel listing of the user window is shown in Figure 4. Following the listing, the consumer creates their personal communal and confidential key.

Figure 4 Screenshot for programming process (see online version for colours)



This section discusses the encryption time, memory and number of data encrypted in proposed technique that means KFCM with double encryption in the authentication process.

Table 1 demonstrates that the encryption time, quantity of data encrypted and encrypted file amount depend on the threshold value are recognised. At this time changeable the threshold value 20 to 100, the data will be encrypted, primarily the data's are measured to the clustering procedure analyse the confidence value. This confidence oriented the data are legitimate by the double encryption procedure. If the threshold is 20 then the encrypted file dimension is 1,521 kb this procedure occupies the encryption time is 15,493 ms it is contrasted to the threshold value 40 the encryption time disparity is 8,424 ms, comparable distinction in the changeable the threshold value among the encrypted file dimension in cloud computing procedure. This table also regards as the

totality amount of data encrypted in entire file dimension, in threshold 40 the encrypted data is 2,728 and its occupied 23,917 ms for encryption procedure. Every threshold value the innovative file dimension is 186 kb to encrypted and decrypted procedure in verification procedure.

Table 1 Encryption in proposed technique for various thresholds

Threshold	*Original file size (kb)*	*Encrypted data*	*Number of data encrypted*	*Encryption time (ms)*
20	186	1,521	130	15,493
40		2,728	263	23,917
60		4,132	417	33,358
80		6,228	647	55,416
100		6,753	705	73,995

Table 2 Time measures in proposed work

Threshold	*Total execution time*	*Encryption time (ms)*	*Decryption time (ms)*
20	19,941	15,493	14,561
40	28,553	23,917	25,642
60	39,200	33,358	31,546
80	60,698	55,416	50,475
100	85,313	73,995	69,413

Table 2 illustrates the threshold value-based entire implementation time, encryption and decryption time of the confidence data legitimate procedure. If the threshold is 20 then the encryption time is 15,433 ms and decryption time is 14,561 ms then the threshold is changeable the encryption and decryption time will be growing. Correspondingly every threshold value the implementation will be intended, this entire execution time depends on the program mining consecutively in software enchanting time in verification effort.

Figure 5 Encrypted file size (see online version for colours)

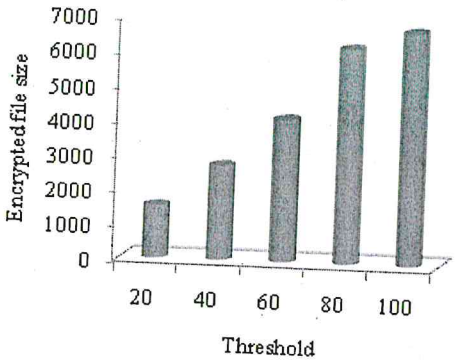


Figure 5 shows for varying the threshold value based on threshold value the encrypted file size are calculated. This graph the threshold is increasing at the same time the encrypted file size is also increasing, if the threshold is 20 the file size is 1,521 it is

compared to the threshold 40 the difference is 1,207 similar difference in other threshold values the encryption file size obtained.

Figure 6 Comparison graph for encryption time (see online version for colours)

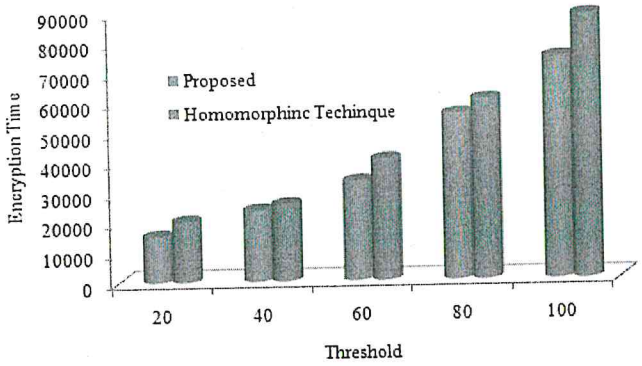


Figure 7 Comparison graph for memory (see online version for colours)

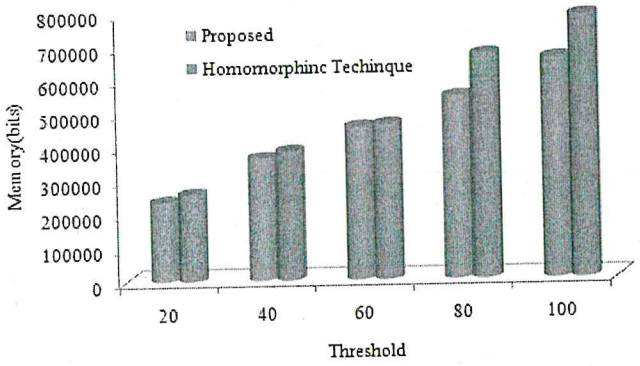


Figure 6 explains the assessment diagram for projected effort and homomorphic encryption procedure the time will be estimated. If the threshold is 20 projected encryption time is 15,493 ms it is evaluated to obtainable homomorphic procedure the distinction is 32.26%. Afterward, the threshold is growing, the projected technique i.e., double encryption procedure created the least encryption time evaluate to the obtainable effort. Figure 7 illustrates the memory assessment diagram for projected and obtainable technique the memory convention of the projected and obtainable facility, average least memory 656,441 bits contrast to the projected progression the distinction is 471,633 likewise to the threshold unreliable procedure.

Figure 8 shows the trust values of proposed and existing approach, since low majority values are chosen, rating credibility suffers low decrement in the case of dishonest ratings from malicious raters. However, in this scenario, the large number of malicious raters directly affects the majority rating and hence the final assessed reputation. Trust accuracy implies the proportion of acquiring right trust an incentive through trust instrument to the total number of assessments. Exchange achievement rate implies the proportion of accomplishment exchanges to the perfect number of exchanges.

Recreation tests reproduced cloud stage that contained 2,000 bunch hubs and 10 put stock in spaces. Every space contains 2,000 asset hubs. Every client hub ought to finish 100 circumstances exchanges arbitrarily with one of the suppliers.

Figure 8 Comparison of trust values (see online version for colours)

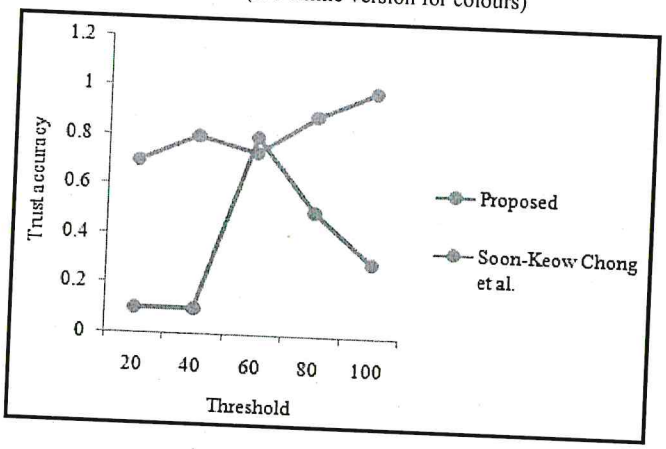


Figure 9 Comparison of clustering approaches (see online version for colours)

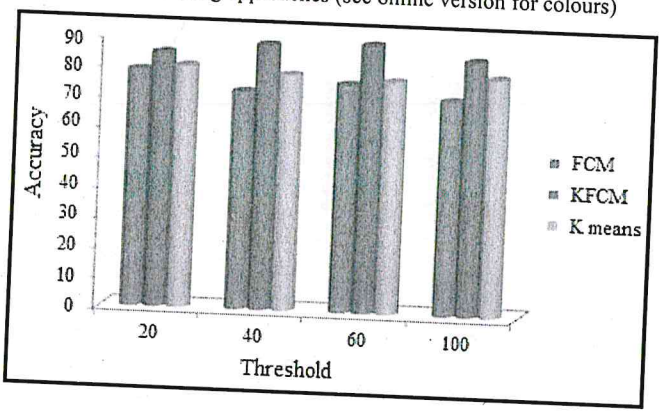


Figure 9 shows the clustering accuracy of the proposed model compared to existing clustering techniques such as FCM and K-means clustering models. Proposed model compared to other technique the accuracy difference is 25 to 30% for all techniques. Benefit requesters will probably acknowledge suggestions from the members who have comparative inclinations to them or from their companions in the informal community from those with whom they do not have any connections. The trust relations between two members can be created in two ways: They have comparative inclinations, and they had coordinate communications before. A trust connection between members is transitive and compostable.

Figure 10 Comparison of trust accuracy (see online version for colours)

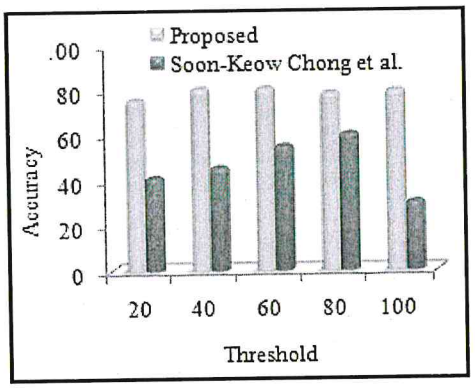


Figure 10 shows when trust value accuracy of service providers is not relevant to the potential transaction. It also shows when service providers are new in the marker with no trust value. The result shows that the proposed model is higher than the trust reputation-based model at the first half of the result. Consequently, all the figures showed that when the percentage of untrustworthy service providers increases the difference value and the maximum accuracy attains 80.51% for threshold values.

5 Conclusions

Shared data values are maintained under third-party cloud data centres. Data values are processed and stored in different cloud nodes. Here the trust-based authentication process clustering and double encryption methods are used. Double encryption process means initially homomorphic encryption used to encrypt the data then this data is processed in blowfish technique to the authentication process. To prove the proposed method achieves better results, the performance of the proposed method is assessed, analysed, compared and contrasted with those of existing (homomorphic encryption) methods. Based on these the quality of our proposed method is proved. From the result analysis, the proposed method proves their effectiveness, analysed the factors and compared with the existing technique. In future, the researcher can carry out their platform with their own optimisation techniques to obtain the optimal centroid in the clustering process.

References

Agre, C. (2015) 'Implementation of a cloud in banking sector', *Journal of Computer Science and Information Technology Research*, Vol. 3, No. 2, pp.1168–1174.

Ahmad, I. and Khandekar, A. (2014) 'Homomorphic encryption method applied to cloud computing', *Journal of Information & Computation Technology*, Vol. 4, No. 15, pp.1519–1530.

Aliahmadipour, L., Torra, V. and Eslami, E. (2017) 'On hesitant fuzzy clustering and clustering of hesitant fuzzy data', *Journal of Fuzzy Sets, Rough Sets, Multisets and Clustering*, pp.157–168, Springer International Publishing.

Bharathia, C., Vijayakumar, V. and Pradeep, K.V. (2015) 'An extended trust management scheme for location based real-time service composition in secure cloud computing', *Proceedings of Computer Science*, Vol. 50, pp.103–108.

Bo, C., Ang, A. and Ao, U. (2014) 'Sar image change detection using regularized dictionary learning and fuzzy clustering', *IEEE 3rd International Conference on Cloud Computing and Intelligence Systems (CCIS)*, IEEE, pp.327–330.

Bose, R., Luo, X.R. and Liu, Y. (2013) 'The roles of security and trust: comparing cloud computing and banking', *Journal of Social and Behavioral Sciences*, Vol. 73, pp.30–34.

Chiregi, M. and Navimipour, N. J. (2016) 'A new method for trust and reputation evaluation in the cloud environments using the recommendations of opinion leaders entities and removing the effect of troll entities, *Journal of Computers in Human Behavior*, Vol. 60, pp.280–292.

Chonga, S.K., Abawajyb, J., Ahmad, M. and Hamidd, I. R. (2014) 'Enhancing trust management in cloud environment', *Proceedings of Social and Behavioral Sciences*, Vol. 129, pp.314–321.

Ciobanu, R.I., Marin, R.C., Dobre, C. and Cristea, V. (2017) 'Trust and reputation management for opportunistic dissemination', *Journal,of Pervasive and Mobile Computing*, pp.1–13.

Fan, W. and Perros, H. (2014) 'A novel trust management framework for multi-cloud environments based on trust service providers', *Journal of Knowledge-Based Systems*, Vol. 70, pp.392–406.

Gong, M., Liang, Y., Ma, J.S.W. and Ma, J. (2013) 'Fuzzy C-means clustering with local information and kernel metric for image segmentation', *Journal of IEEE Transactions on Image Processing*, Vol. 22, No. 2, pp.573–584.

Gupta, B.B. and Badve, O.P. (2015) 'GARCH and ANN based DDoS detection and filtering in cloud computing environment', *IEEE 4th Global Conference on Consumer Electronics (GCCE)*, IEEE, pp.1–5.

Gupta, B.B. and Badve, P.P. (2016) 'Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a cloud computing environment', *Journal of Neural Computing and Applications*, pp.1–28.

Habib, S.M., Ries, S. and Mühlhäuser, M. (2010) 'Cloud computing landscape and research challenges regarding trust and reputation', *Proceedings of Intelligence & Computing*, pp.410–4116.

Huang, J. and Nicol, D. (2013) 'Trust mechanisms for cloud computing', *Journal of Cloud Computing: Advances, Systems, and Applications*, Vol. 2, No. 9, pp.1–14.

Khan, S.S. and Tuteja, R.R. (2015) 'Security in cloud computing using cryptographic algorithms', *Journal of Innovative Research in Computer and Communication Engineering*, Vol. 3, No. 1, pp.148–154.

Kretzschmar, M. and Golling, M. (2011) 'Security management spectrum in future multi-provider inter-cloud environments – method to highlight necessary further development', *Proceedings of Systems and Virtualization Management*, pp.1–8.

Krishna, R.S., Sayi, T.J.V.R.K.M.K., Mukkamala, R. and Baruah, P. K. (2012) 'Privacy-preserving data management in mobile environments: a partial encryption approach', *Proceedings of Mobile Data Management (MDM)*, pp.167–175.

Kumar, K. and Jain, A. (2015) 'Trust enhancing model for cloud environment', *Journal of Computer Applications*, Vol. 131, No. 5, pp.36–40.

Li, J., Zheng, X., Chen, D. and Song, W. W. (2012) 'Trust based service selection in service oriented environment', *Journal of Web Services Research*, Vol. 9, No. 3, pp.23–42.

Li, W., Ping, L. and Pan, X. (2010) 'Use trust management module to achieve effective security mechanisms in cloud environment', *Proceedings of Electronics and Information Engineering*, Vol. 1, pp.14–19.

Lughofer, E. and Pratama, M. (2017) 'On-line active learning in data stream regression employing evolving generalized fuzzy models with certainty sampling', *Journal IEEE Transactions on Fuzzy Systems*, pp.1–5.

Lughofer, E., Cernuda, C., Kindermann, S. and Pratama, M. (2015) 'Generalized smart evolving fuzzy systems', *Journal of Evolving Systems*, Vol. 6, No. 4, pp.269–292.

Martucci, L., Zuccato, A., Smeetsk, B., Habib, S., Johansson, T. and Shahmehri, N. (2012) 'Privacy, security and trust in cloud computing the perspective of the telecommunication industry', *Proceedings of Intelligence and Computing and 9th International Conference on Autonomic and Trusted Computing*, pp.627–632.

Negi, P., Mishra, A. and Gupta, B. B. (2013) 'Enhanced CBF packet filtering method to detect DDoS attack in cloud computing environment', *Journal of arXiv preprint arXiv: 1304.7073*, pp.1–5.

Pawar, J., Kumbhar, V. and Bhat, S. (2014) 'Study & comparative analysis of different algorithms used in data security in cloud environment', *Journal of Management and Computer Application*, pp.76–80.

Pratama, M., Anavatti, S.G. and Joo, M. (2015a) 'pClass: an effective classifier for streaming examples', *Journal of IEEE Computational Intelligence Society*, Vol. 23, No. 2, pp.369–386.

Pratama, M., Lu, J. and Zhang, G. (2015b) 'Evolving type-2 fuzzy classifier', *Journal of IEEE Computational Intelligence Society*, Vol. 24, No. 3, pp.574–589.

Pratama, M., Er, M.J., Anavatti, S., Lughofer, E., Wang, N. and Arifin, I. (2014) 'A novel meta-cognitive-based scaffolding classifier to sequential non-stationary classification problems', *IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)*, pp.6–14.

Pratama, M., Anavatti, S. and Lu, J. (2016a) 'Recurrent classifier based on an incremental metacognitive-based scaffolding algorithm', *Journal of IEEE Transactions on Fuzzy Systems*, Vol. 23, No. 6, pp.2048–2066.

Pratama, M., Lu, J., Lughofer, E., Zhang, G. and Er, M.J. (2016b) 'Incremental learning of concept drift using evolving type-2 recurrent fuzzy neural network', *Journal of IEEE Computational Intelligence Society*, p.1.

Pratamaa, M., Lua, J., Anavattib, S., Lughoferc, E. and Lim, C. P. (2016c) 'An incremental meta-cognitive-based scaffolding fuzzy neural network', *Journal of Neurocomputing*, Vol. 171, pp.89–105.

Pratamaa, M., Lub, J., Lughofer, E., Zhang, G. and Anavattid, S. (2016d) 'Scaffolding type-2 classifier for incremental learning under concept drifts', *Journal of Neurocomputing*, Vol. 191, pp.304–329.

Pratama, M., Lughofer, E., Lim, C.P., Rahayu, W., Dillon, T. and Budiyono, A. (2016e) 'pClass+: a novel evolving semi-supervised classifier', *Journal of Fuzzy Systems*, Vol. 19, No. 3, pp.863–880.

Saeed, M.Y. and Khan, M.N.A. (2015) 'Data protection techniques for building trust in cloud computing', *International Journal of Modern Education and Computer Science*, Vol. 7, No. 8, p.38.

Shaikha, R. and Sasikumar, M. (2015) 'Trust model for measuring security strength of cloud computing service', *Journal of Computer Science*, Vol. 45, pp.380–389.

Shereek, B.M., Muda, Z. and Yasin, S. (2014) 'Improve cloud computing security using RSA encryption with Fermat's little theorem', *Journal of Engineering*, Vol. 4, No. 2, pp.1–8.

Singh, S. and Sidhu, J. (2017) 'Compliance-based multi-dimensional trust evaluation system for determining trustworthiness of cloud service providers', *Journal of Future Generation Computer Systems*,Vol. 67, pp.109–132.

Sirohi, P. and Agarwal, A. (2015) 'Cloud computing data storage security framework relating to data integrity, privacy and trust', *Proceedings of Next Generation Computing Technologies*, pp.115–118.

Srisakthi, S. and Shanthi, A.P. (2015) 'Towards the design of a secure and fault tolerant cloud storage in a multi-cloud environment', *Information Security Journal: A Global Perspective*, Vol. 24, Nos. 4–6, pp.109–117.

Stergioua, C., Psannisa, K.E., Kimb, B.G. and Guptac, B. (2016) 'Secure integration of IoT and cloud computing', *Journal of Future Generation Computer Systems*, pp.1–25.

Suna, D., Changb, G., Suna, L. and Wang, X. (2011) 'Surveying and analyzing security, privacy and trust issues in cloud computing environments', *Procedia Engineering*, Vol. 15, pp.2852–2856.

Tang, C. and Liu, J. (2015) 'Selecting a trusted cloud service provider for your SaaS program', *Journal of Computers & Security*, Vol. 50, pp.60–73.

Tanga, M., Daia, X., Liua, J. and Chen, J. (2016) 'Towards a trust evaluation middleware for cloud service selection', *Journal of Future Generation Computer Systems*, Vol. 74, pp.302–312.

Varalakshmi, P. and Judgi, T. (2016) 'Multifaceted trust management framework based on a trust level agreement in a collaborative cloud', *Journal of Computers and Electrical Engineering*, Vol. 59, pp.110–125.

Venkatesan, R., Er, M.J., Pratama, M.D. and Wu, S. (2016) 'A novel online multi-label classifier for high-speed streaming data applications', *Journal of Evolving Systems*, pp.1–13.

Wang, H. and Wang, J. (2014) 'An effective image representation method using kernel classification', *Proceedings of Tools with Artificial Intelligence*, pp.1–6.

Yamad, A. and Ikeda, T. (2017) 'Enhanced PKI authentication with trusted product at claimant', *Journal of Computers & Security*, Vol. 67, pp.324–334.