Chapter 9
Design of a Confidentiality Model Using Semantic-Based Information Segmentation (SBIS) and Scattered Storage in Cloud Computing

N. Thillaiarasu, Naveenbalaji Gowthaman, and S. Chenthur Pandian

9.1 Introduction

For imposing a vibrant safety concern the intention is to design a confidentiality prototype that provides a pre-planned confidentiality assurance for assuring its probability for which the proposal of empirical schemes reduces the number of cloud storage positions for depicting their abilities and precisely they are used for the least designed and most exciting information varieties.

9.1.1 Organization

This work has been organized as follows: Sect. 9.2 prefaces the work carried out; Sect. 9.3 has details about the general information about the work; Sect. 9.4 describes the contributions carried out to implement the new idea proposed in this work; Sect. 9.5 tells about the safety protocols used in the extensive design of this work; Sect. 9.6 describes the method of safeguarding the data collected without compromising the confidentiality in the cloud framework; Sect. 9.7 tells about the subcontracting of information with confidentiality assurance using background refinement and semantic data segmentation; Sect. 9.8 tells about the experimental

N. Thillaiarasu
School of Computing and Information Technology, Reva University, Bengaluru, India

N. Gowthaman (✉)
Department of Electronic Engineering, University of KwaZulu-Natal, Durban, South Africa

S. Chenthur Pandian
Department of EEE, SNS College of Technology, Coimbatore, India

S. Nath Sur et al. (eds.), *IoT and IoE Driven Smart Cities*,
EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-82715-1_9

analysis carried out; Sect. 9.10 discusses about the result with comparisons; Sect. 9.11 summarizes the work carried out; and Sect. 9.11 concludes the work with future establishments.

9.2 Preface

Cloud computing provides several profits to firms, public sectors, and people interested to store and process their information into the cloud such as vigorously expendable supplies, enhanced quickness, and administered, expandable, accessible, and global information available freely without bothering the topographical positions which offers estimation supremacy and elasticity [1]. Precisely cloud computing commonly makes use of cost cutdowns because it minimizes the prototypes and cost for preservation which thereby offers inexpensive storage abilities and analysis [2]. Precisely the intention is to design a semantic-based information segmentation that is capable of mechanically identifying information chunks that might create danger and divides them from the restricted principles so that every segment does not face any possible threats followed by which the segments of the flawless information are freely stored into individual positions of a multi-cloud so no peripheral objects can gain access to the comprehensive private information [3–5].

It is to be noted that the fractional information is stored in vibrant cloud environments; the outsourced characteristics are effortlessly and effectively aided by distributing the requests to several cloud positions. For imposing a vibrant safety concern the intention is to design a confidentiality prototype that provides a pre-planned confidentiality assurance for assuring its probability for which the proposal of empirical schemes reduces the number of cloud storage positions for depicting their abilities and precisely they are used for the least designed and most exciting information varieties [4].

Since the safety-related issues regarding information outflow is focused due to the missing straightforward mechanism over the storage and administration of the subcontracted information which experiences diverse risks retarding several users from transfer their data to the cloud environment. In the European Union, nearly 40% of firms are making use of the cloud which conveys the threats in safety-related breaks as the key restricting feature in making use of cloud-related services. Precisely in the article released by the cloud safety association over nearly 170 IT and security experts in the United States several defendants measured cloud storage as an immense hazard. The European Network and the information safety assistance recognized missing control over the information subcontracted to the cloud as an unsympathetically significant feature.

For instance, *Dropbox* is meant to be an encoder for the user information by making use of dense cryptographic schemes where the private keys are generated and administered by the *Dropbox* themselves and not by the creator of the information [5]. Furthermore, the present safety-related issues negotiate information of users to store their information in the cloud. Several reputed illustrations comprise Sony Play Station outages due to the peripheral invasions where the private information from nearly 77 million user accounts was taken where the multiday outages in *Dropbox* momentarily permit the guests to gain access into desired files of their 25 million user accounts which might create malformation disputes or outflow of confidential pictures stored into the storage services of cloud.

Moreover, the use of the cloud might have disquieted the cloud service supplier's focus on processing their information. Cloud computing offered service providers the chance for examining and making use of the immense volume of secret information; for instance, the current confidentiality-related rule in Google states all the prevailing data which the user desires to distribute by Google to enhance or advertise its services. Likewise, Yahoo also attempts to gather precise user information and make use of them by aggregating them with the data acquired from the corporate companions. The information gathered by the service suppliers could be employed to aid the users but in parallel, it might create disputes related to confidentiality [6, 7]. Based on the documents provided by the Federal Commerce Directives it is postulated that the service providers often gather and examine the users' information without the awareness of the users and some references to these study can be profound; for instance the service suppliers can locate the data regarding diabetes since their attention is towards the gluten-free products and then distribute this data with the insurance firm which could make use of this data for categorizing the individual to be in an immense danger. In the financial concept the automated information is often regarded as the fresh input where the intention of the users is regarded as the information-processing activities accomplished by the service suppliers which are comprehensible and logical [8].

To overcome the issues and to recoup the user mechanism over the safety employed to the private and subcontracted data over-the-cloud diverse schemes are designed. The intention was to make use of precise sort of information safeguarding on the user side so that only safe results are subcontracted to the cloud which thereby permits only the creator of the information to precisely rebuild the information acquired from the cloud.

9.3 Genesis

Encoding is a normal solution for imposing information safety in cloud computing. Diverse solution mechanism is based on public and linear key cryptographic schemes are designed for storing information in the cloud where information safety is offered using encoding. The encoding is accomplished before the information is communicated and stored in the cloud and it is decoded only after that information is reverted to the creator of the information. These solutions are normally imposed as a belief-based encoding process; for instance, the cipher cloud offers a safe entry positioned in a belief environment besieged by diverse prevalent *SaaS* service suppliers [9–11]. It makes use of encoding to precise user-related information very before storing this information in the cloud. The cloud service is duplicated in the safe entry to offer logical outcomes to the processes such as investigation or categorization. The encoded keys are arranged and stored nearby under the influence of the user. The viewpoint system makes use of the identical mechanism which holds a server and a rear proxy that executes information encoding schemes. The safe cloud is a perfect solution for *IaaS* which is a cloud-based implementation platform where the application data are stored and encoded within the cloud, thus departing the initial governance and the description of access rules to the users.

Though the aforementioned system provides confidentiality safeguarding information storage for the users they experience diverse issues either mechanically or in the user base. The transmission between the service suppliers and the client device is seized and back processed for improving its safety aspects which are translucent to both the service suppliers and the users. However the transmission standards might frequently alter which thereby needs a consistent revision of the offered safety aspects which is a complex process that can extremely damage the dependability and accessibility of the services. Moreover, the service suppliers may execute precise countermeasures to avert these schemes in rough situations where the users analytically upload encoded contexts to their servers. It is precisely applicable to the service suppliers which offer services without involving costs since they anticipate acquiring turnover based on the user's information which might prohibit users from providing only encoded and unusable information [11].

The delicate data are analytically encoded and stored by the service providers which are intended to be conscious about the features provided by the service suppliers which could produce drivel results. Here only a minimized set of features are safeguarded or encoding could only be applied to that information that is not operated by the cloud or the cloud services that might be duplicated are the reliable entry. Lastly, the entry is enforced to excessively store plain information and to re-execute along with the back processing of several cloud services, thereby overcoming the comprehensive intention of information and evaluation subcontracting [12]. Though presently the cryptographic-based solutions are designed with restricted aids for several processes over the encoded information, the intricate process will need addressing mechanisms from identical encoding which are quite effectively used for real-time applications. There are more effective locatable encoded solutions which need appending of a substantial volume of information to the subcontracted information accomplishing diverse requests for reviving the harmonized information and provide restricted help for intricate and linked requests comprising rational and relation-based operators along with the value extremes.

The encoding of comprehensive information uploaded to the service suppliers at the client side suggests the forfeiture of diverse levels of direction effectively in terms of both the storage and processing which in the context of cloud computing depicts crushing its individual goal since one of the key intentions for migrating to the cloud is to cut down the cost. Furthermore, the supervision of encoded key might append fresh safety-related threats at the user side [12, 13].

The immense ranges of users are not aware of the basic conception of the cryptographic schemes and several of them cannot correctly govern the keys which thereby negotiates the efficiency and safety due to the inattentive administration of cryptographic schemes. For addressing these issues the intention is to design confidentiality safeguarding schemes alternate to the information encoding which governs the information more precisely [14]. To impose it becomes mandatory to be dependent on the immensely progressing context of multi-clouds, i.e., the usage of diverse cloud computing services in a unique individual framework. The multi-cloud appends diverse merits like minimized dependencies on any particular seller, thus escalating the suppleness or justifying the tragedies, but the focus is upon the scattered and independent nature of multi-cloud services. It paves the way for alternate information safeguarding schemes based on the information segmentation or divisions.

With information segmentation, the delicate information within a document or prevailing within the repository is divided into segments and stored in individual places so that every distinct segment does not reveal their individualities or any private data. Particularly the scattered storage of segments minimizes the volume of data acquired by the third party who adapts the data gathered from the information examination or user summarization becomes partial and unclear which also reduces the concerns of possible breaks. Likewise, the intention is that the information is stored in a precise manner which makes it probable to effortlessly recollect the number of cloud features by distributing the user requests since they are made use in fractional information segments which makes it probable for the information creator with the knowledge of position related to every segment for rebuilding the comprehensive outcomes by aggregating and uniting the fractional outcomes in a process with more efficient information decoding [15].

Thus on evaluation with information encoding and aiding an immense diversity of features the information segmentation does not face immense overheads linked with processing the requests. Lastly, in conditions where the service suppliers anticipate non-encoded information about the unique segments, it might be helpful since the service suppliers could still accomplish information examination and revive fractional inferences [7, 15, 16].

Diverse segmentation mechanisms are designed over decades which intend to perform information segmentation in a binary fashion. For instance, the users are segmented into bytes which are transferred and rejoined into a static set of segments which are lastly stored in different positions. Each of the subcontracted files is linked to an initial level which is selected by the users based on the compassion of their contexts. Then the segments are generated based on the RAID protocol storage schemes and those with utmost levels of confidentiality are stored in positions where the user relies on. These schemes where the information is segmented are performed following the static conditions and bytes are chosen in alternate and rejoined and are employed for comprehensive binary or even hypermedia files where the contexts are normally stored but not operated by the cloud schemes [8, 9, 13, 16].

Therefore files with contexts shall be operated by the cloud schemes for offering the features where the created outcomes provide neither confidentiality nor service assurance. Moreover, it is not probable to assure that segments of bytes do not hold adequate information to create exposure in case if it is too huge and not probable to assure cloud features or retains fractional information used for the service suppliers in case the segments are too minimal or partially joined. It makes it too complex for the users to comprehend safety and service conservation for which a precise scheme is made use of which naturally is dependent on the semantics of the information to be safeguarded [15–17].

At the elementary level, all the information segmentation schemes are intended on the planned repositories. In these situations, the information segmentation could be flat or upright. Therefore as per the statement, the flat segmentation is of restricted use in allowing confidentiality safeguarding and breakdowns since the revealing is often created from the synchronization among the entities instead of diverse documents which are normally autonomous. The upright segmentation is designed for assuring privacy at the documentation level by locating the entities of the repository which are encoded; meanwhile the quasi-identifiers are segmented and stored in diverse places [17]. Both the schemes restrict the number of positions since they consider that there is an individual set of quasi-identifier-based entities. Likewise, the exposure is sidestepped along with the preservation of information utilization at the entity level. Furthermore, the intention is to design diverse schemes for deciding the best breakdown for reducing the expenses of the following SQL requests which require being scattered and their outcomes are combined.

Though these schemes provide more vigorous assurances and improved features than the binary schemes they firmly depend on the modeling of information and on a set of physically described policies that state the groups of entities that might create breakdowns and segmentation [18]. Consequently, it could be operated to the unplanned information like documents and might not expand with immense information sets since human involvement is required to describe the uncertain mixture of entities for every information set. Furthermore, it is recognized by describing these dangerous mixtures which are an expensive and intricate process even for professionals.

9.4 Contributions

For addressing the restrictions of afore-detailed issues the intention is to design semantic-based information segmentation and safeguarding schemes for the subcontracted information prevailing over the cloud. The designed scheme aims to evaluate the original semantics of the information to be safeguarded and the confidentiality prerequisites of the users for mechanically identifying the information segments which might create breakdowns and mechanical organization of segmented information to assure confidentiality to the user. In contrast to the schemes of information segmentation at the binary level the designed schemes segment the information along with the scattering of information contexts and the confidentiality prerequisites of the user. Thus the context of the resulting segments is not linear and is assured that it does not create any breaks in terms of confidentiality

[18, 19]. It is also compared with the schemes where the concern is on entailing privacy of user precise information.

The prevailing solution might be impractical for several conditions for the immense volume of documents that are subcontracted to the cloud system and the missing data of several users regarding the confidentiality hazards bothers their possessed information. Lastly, the comparison of methods based on the planned repositories in the designed scheme is uniquely based on the information semantics and it can make use of any variety of information irrespective of not focusing on their frameworks. To state the abilities and overview of the designed scheme, the intention is on the storage of fresh text-based documents where the most intricate task is to safeguard their absence of framework where similarly they comprise the most mutual manner to interchange possibly delicate data among the human players [20].

The goal of the designed scheme is stimulated from the conventional document purification schemes which endeavor at mechanically locating and safeguarding delicate elements in the input documents. To offer a pre-planned confidentiality assurance, the designed scheme satisfies an integral semantic-based confidentiality prototype for safeguarding documents. Based on the statement and imposing of confidentiality prototypes the information creators could innately describe their confidentiality prerequisites based on the semantics of the information which they do not wish to reveal to the cloud and possible intruders.

9.5 Safety Prototypes and System Framework

The designed safety prototype in which the user does not have belief in any service suppliers to safeguard their data. It is also regarded that all the service suppliers are truthful but could be probing; that is, it might assemble, process, and examine the information stored along with the requests they acquire from the users. It anticipates acquiring extra user information or breach any safety extents that the users might have executed over the information preceding subcontracted them. For any service supplier as a profitable supplier of services, it would not perform malevolently against the users and would precede the standards as anticipated, i.e., being truthful. It is also regarded that the accessibility of diverse service providers offering individual services, i.e., multi-cloud and providing a group of places where the information is possibly stored. It is also noted that the diverse service providers are autonomous from one another which does not allow to combine the fractional information that is stored to break down the user confidentiality [17–21].

Lastly, it is regarded that the user side is comprehensively believed and safe since it is the location where the information is stored preliminarily. Since it could be made use in a limited application or as a proxy on the user side it could safely process the flawless information preceding subcontracting them to the cloud and stores this metadata required to process the following requests on that information and rebuild the outcomes. For some situations, these safe applications or proxies can

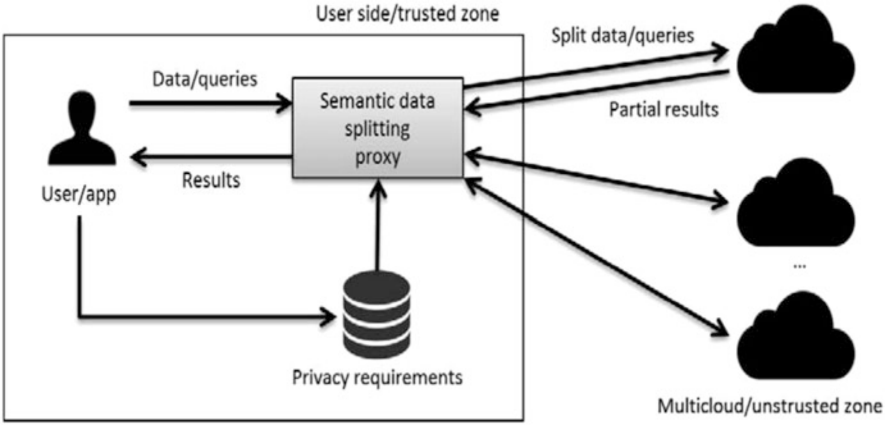

Fig. 9.1 General framework of the system

be distributed among diverse users. Here the cloud storage places will be distributed among diverse users. The application-level proxies would preserve the group of prevailing cloud places visible to the users [19, 21].

Furthermore, the users might state a set of confidentiality prerequisites that describe the theme which shall be safeguarded in any subcontracted information over the cloud, i.e., the utmost level of semantic exposure the user is permitting for every context. The prerequisites might be linked to the individualities needing safety against the revealing of uniqueness or private information, i.e., the entity revealing. In comparison to the prevailing schemes, these prerequisites are described at the abstract level instead of at the planning level. Based on the conditions entailed above, the framework is depicted in Fig. 9.1.

In semantic-based information segmentation, the proxy accomplishes two key activities, namely storage of information within the cloud and retrieval of information from the cloud as the outcome of the user request. The logic prevailing on the initial activity is portrayed in Fig. 9.2. Initially, the proxy acquires the information to be stored and makes use of discovery possibilities of the context. Performing these is dependent on the safety prerequisites entailed by the user so that the existence or synchronization of the input information might disrupt the confidentiality of the users which are spontaneously labeled as hazardous. This labeled information is then conceded to the segmentation component which consequently is hazardous and the limitations described in the confidentiality prerequisites make choices on the mechanism that the information is segmented and storage place required so that every chunk of information could be securely hoarded and compositely termed as information segments. It also stores the segmentation conditions within the local repositories as metadata so that the system could function flawlessly and processes the future requests over the information and combines the fractional outcomes followed by which they transmit every information segment to discrete service suppliers [22].

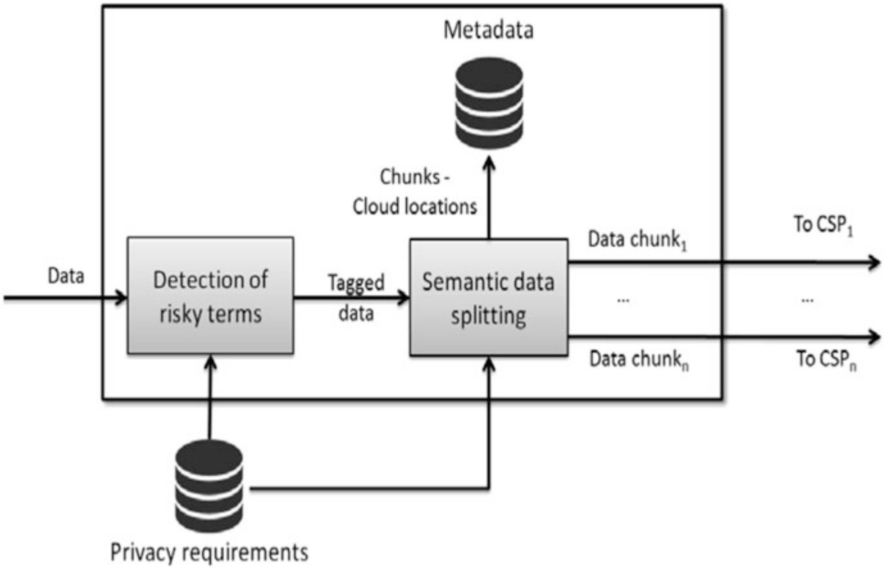

Fig. 9.2 Information subcontraction workflow to the multi-cloud through semantic-based information segmentation

Likewise, it is assured that the segmentation process is away from losses; that is, it offers a chance for rebuilding the actual outcomes in case if there is no need to store the comprehensive information within the local locations and the confidentiality-safeguarded contexts are stored in every isolated service suppliers that do not experience risks about safety prerequisites of the users [22]. In case if diverse users make use of identical proxy and distribute an identical group of cloud positions each position might hoard segments of flawless information from diverse users; that is, the segmented information of diverse users is multipart at each cloud location.

Since the proxy is the only probable understanding of segments related to the users offering an extent of safety against the approval of diverse service suppliers, the latter might limit the attempts to combine the fractional information they hoard which in turn are nosedived since they cannot differentiate the users to the matching information segments. Likewise, the reasoning linked to the implementation of user requests over the subcontracted information and the combination of concluding outcomes is portrayed in Fig. 9.3. Initially, the request is processed in the order that the storage positions of the information and the requests infer to the retrieval from the local metadata repository. Following this the requests are duplicated sometimes as the information segments are divided and the requests are transmitted to the resultant service suppliers. Consequently, the service suppliers offer a set of outcomes that depict a fractional vision of the comprehensive outcomes [20–23]. Lastly, the proxy combines these outcomes with the conditions employed to segment

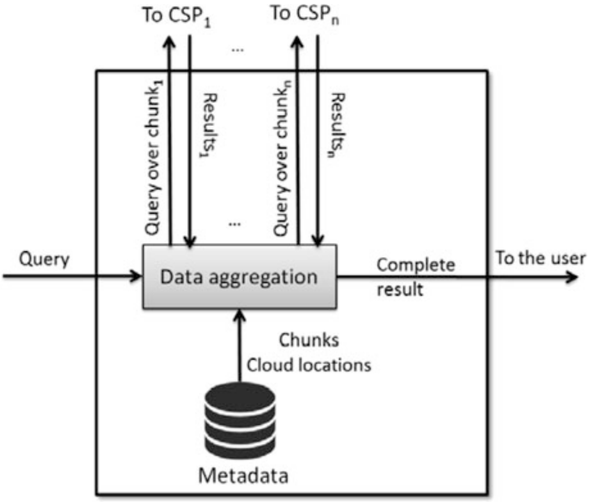

Fig. 9.3 Request-reply workflow with the segmented information

them and also stores them as metadata and offers comprehensive outcomes to the user.

9.6 Safeguarding Information Without Negotiating Confidentiality

There are diverse confidentiality schemes designed by several scholars to provide rigorous confidentiality assurances for safeguarding information. Many of these schemes like k-secrecy schemes along with their addition to plain text-based documents achieve the standard arrangement of the information for describing the confidentiality possibly as re-recognition of an individual within the information set to be unconfined [23]. Confidentiality is thus imposed by making the person vaguely recognize the information within the information set; that is, it primarily safeguards the information against self-exposure.

The other prevailing frameworks like differential confidentiality deal with the planned information sets and needs elements with restricted areas. Therefore the documents are created freely by every user and they shall be safeguarded exclusively based on the semantics they expose where open texts are also unplanned and limitless. Furthermore, the illustration of confidentiality prototypes is natural so that it could be used by the users to precisely describe their confidentiality prerequisites, and diverse confidentiality prototypes are created based on intangible numerical which several users feel too intricate to understand [24]. Lastly effortless aids are offered for safeguarding against self or entity exposures.

The only confidentiality prototypes which are suitable for these circumstances and prerequisites are background refinement which is a common confidentiality prototype for text-based refinement. The background refinement describes the preferred level of confidentiality in terms of a set of contexts in a manner that the confidentiality assurances are satisfied if the safeguarded results do not hold any of these terms which uniquely or jointly exist within the same documents, thus revealing the semantics of the delicate elements [25]. For instance in medical documents the HIV and AIDS refined form shall not hold these terms because the illegal information stealer might gain access to the safeguarded documents relating to AIDS and HIV. The prototype is described below.

9.6.1 Illustration 1 (Background Refinement)

For an input document id, the contextual information i_c prevails for the possible intruders where a set of delicate information d_i has to be safeguarded. It is depicted that id' is the background refined version of id if and only if id' does not hold any of the word w or set of words w_s which individually or in combination could expose any of the units within background refinement by negotiating i_c. For precisely arranging the transaction in between the extent of safety and information utilization it is possible to describe a fixed value of extreme expose by mentioning a set of overviews $O(d_i)$ for the delicate objects. For instance, the (HIV, sickness) and (HIV) refined document will not only retard exposure of AIDS but also expose those contexts related to an ailment and virus correspondingly.

9.6.2 Illustration 2 ((d_i, $O(d_i)$)) Refinement

For a given input document id the background data i_c is a well-ordered set of delicate objects d_i to be safeguarded along with the arranged set of their related overviews $O(d_i)$. It is inferred that id' is the ((d_i, $O(d_i)$)) refined version of id if and only if i_d' does not hold any word w or set of words w_s which solely or jointly exposes more semantics in all i_c offered by their particular $O(d_i)$ by negotiating d_i. Based on the illustration in the background refinement prototype, the users could describe their confidentiality prerequisites due to the metrics d_i in terms of semantic tags which is a set of delicate contexts that the safeguarded documents will not expose. Another key merit of the prototype is that it could be simply depicted to impose the confidentiality prerequisites of the prevailing regulation and principles on the confidential information whose descriptions related to the delicate information are also semantic.

Lastly, the utilization of overviews $O(d_i)$ as exposed fixed values for d_i authorizes to the minimal volume of semantics that could be exposed related to d_i which imposes the system to execute a sterner refinement. In terms of semantics, the utilization of overviews in the model depiction is to excellently tune the confidentiality assurances naturally and to offer a clear insight on the volume of data that the peripheral objects could acquire from the safeguarded document.

9.7 Subcontracting of Information with Confidentiality Assurance Using Background Refinement and Semantic Data Segmentation

The intention is to describe the semantic-based information segmentation scheme which is linked with information segmentation for mechanically coordinating the segmentation process and the forthcoming requests along with information revival based on the semantics and threats related to confidentiality of the information [26, 27]. To provide confidentiality assurance the safety is provided by the designed schemes which satisfy the background refinement process similar to the segmentation and scattered storage of segments in isolated service suppliers which are accomplished based on the semantics and sensitivity of the document contexts and confidentiality prerequisites of the user in a manner in which the segments that are stored individually in the cloud do not face any issues related to confidentiality negotiation.

The comprehensive process is accomplished in two ways as identification of words within the input document creating exposure threats based on the confidentiality prerequisites and segmentation along with transmitted storage of words for retarding exposures.

9.7.1 Identification of Precarious Words

The dynamic identification of precarious words happening within the input document is motivated by the concept of exposure entailed by the depiction of background repetition prototype which entails the confidentiality prerequisites. The semantic exposure that the words w/w_s created concerning the elements to be safeguarded d_i could be certainly imposed with data in terms of the hypothesis by calculating the volume of data given by w/w_s about d_i. The semantics covered by the element d_i could be refined based on its data context d_i similar to the semantics that a term w or a set of words w_s reveals regarding the object d_i which is measured based on the point-based synchronized data PSD (d_i,w). Therefore it is possible to recommunicate the common description 1 as entailed below.

9.7.2 Illustration 3 (Data Hypothesis for Background Refinement)

For the input document id, the contextual information i_c and a set of delicate information d_i have to be safeguarded for which it is portrayed that i_d' is the background refined version of i_d if and only if for all d_i, i_d' does not hold any words w or set of words w_s based on i_c as PSD $(d_i,w) = d_i$ (or) PSD $(d_i,w_s) = d_i$ correspondingly.

Based on the condition the words w or a set of words w_s within the input document where PSD $(d_i,w) = d_i$ (or) PSD $(d_i,w_s) = d_i$ for any d_i in d_i' will create threats related to exposure. The d_i of an object d_i estimates the data/semantics which should be concealed due to their delicate nature where the PSD estimates the volume of data/semantics that a word w or set of words w_s should disclose about d_i. Figure 9.3 depicts the association between d_i and PSD where cancer is considered to be objected d_i to be safeguarded and operation is the term w happening within the document which is semantically associated with d_i. The figure portrayed in grey exposes the data/semantics in which w creates d_i [24, 28].

The threats related to exposure and its estimation can be elaborated if the overviews of the delicate objects $O(d_i)$ are described as the fixed value of utmost exposures. Based on the changes performed in description 2 in the data hypothesis the threats related to exposure occur for those words w or a set of words w_s within the input document where PSD $(d_i,w) > d_i$ (or) PSD $(d_i,w_s) > d_i$ for any d_i in d_i'.

For real time d_i is evaluated as the reciprocal of the likelihood of its existence:

$$d_i = -\log 1\,(d_i) \tag{9.1}$$

The likelihood required to estimate the data related to the text is normally evaluated which generates minimal data than the precise ones since the likelihood of arrival in the exposure of proceeding is higher [3, 11, 21–23, 27, 28].

Similarly, the PSD (d_i,w_s) is estimated as the normalized likelihood of synchronized d_i and $w = \{w_1, \ldots.., w_n\}$ given their combined and border likelihoods:

$$\mathrm{PSD}\,(d_i, w_s) = \log\left(\frac{l\,(d_i, w_1, \ldots, w_n)}{l\,(d_i)\cdot l\,(w_1, \ldots, w_n)}\right) \tag{9.2}$$

To seize the accurate perception of exposure, the likelihood of its existence shall be estimated from a quantity that openly symbolizes the information i_c prevailing to the probable intruders to accomplish their interfaces [29]. Therefore in worst-case conditions, the quantity shall be huge and is varied enough to shield and seize the data broadcasting at a common balance. The Internet is well matched for serving the purpose because it provides an immense volume of straightforwardly reachable data/awareness sources and it is immense that it is varied for a real-time proxy for social information. Furthermore, the scheme likelihoods could be estimated effectively by requesting words and a set in openly prevailing Internet-based search engines and estimating the resultant page calculations:

$$l(w) = \frac{Web\_Page\_Calculation}{Overall\_Webs} \tag{9.3}$$

Here the overall Webs are the number of prevailing Web resources filed by the Internet-based search engines. The design of Internet-based data and evaluation of exposed threats for identifying the precarious words at the proxy connected at the user side is carried out [29]. The below-entailed routine executes the operation.

9.7.3 Algorithm: Identification of Precarious Words

```
id = id′
di = acquire suspicious grouping
if (di = = 1)
substitute (di, id′)
hd = acquire most helpful data
while (di!=0)
position_identification = false
data_chunk = initial
while (not (position_identification) && (data_chunk ≠ null))
hd = data_chunk + hd
if (not (verify exposure (safe ordered elements, helpful data)))
position_identification = True
append (hd, data_chunk)
eradicate (hd, di)
di = create rest of the terms
else
data_chunk = next (data_chunk)
end if
end while
```

9.7.4 Semantic-Based Information Segmentation and Scattered Storage

For the concept of document refinement, the input documents in its safeguarded form shall be unrestricted based on packets where the words are identified as threats that are normally detached so that the extent of exposure it create; is minimized below the confidentiality prerequisites [30]. It creates a loss of usage because some of the actual words are not prevailing within the detailed procedure within the safeguarded results.

Within the multi-cloud storage conditions conversely, it is possible to gain merits of the prevailing diverse cloud storage positions to divide and store precise information within the confidentiality-safeguarded manner while recalling most of the subcontracted features. Due to diverse cloud storage positions, it is not conscious about one another nor segmented conditions executed by the local proxy as the service suppliers will not be able to rebuild the comprehensive information in a clear manner that retards the exposure [30, 31]. Furthermore, because single-cloud positions are accessed by diverse users due to their scattered nature it is governed by the proxies; the segmented chunks of each user are combined which appends the arbitrariness of the subcontracted information stored at each position and provides an improved safety against conspiracy threats of diverse service suppliers that might attempt to combine incomplete information segments.

For some conditions and inconsistency with the background refinement, the confidentiality prototype on which we are dependent for the segmentation process shall assure that every individually stored information segment satisfies the descriptions 1 to 2 hypothetically using their data. Based on the uncertain words the precarious words identified within the preceding phase might vary in two cases. Initially, the location of separate words w for unique existence within the document creates exposure threats based on the confidentiality conditions [11, 24, 30]. For instance, for acquiring a medical record to be cancer refined the individual existence within the document of replacements of cancer such as malevolent neoplasm or the specialties like breast cancer comprehensively reveals the semantics of the word cancer.

Furthermore, in the usage of overviews of cancer to set severer confidentiality conditions for the model illustration other discrete words might also create exposure. For illustration within a refined document, any knowledge of ailments is also an overview of cancer such as a tumor which might also cause exposures [31]. These unique words could also be regarded as recognizers to the units to be safeguarded and they shall be stored in a precise form within any cloud location. These words as entailed lastly symbolize a minimal volume of data that should be safeguarded and stored locally by the proxy.

It is possible to recognize the mixture of words PWs = $\{w_1, \ldots, w_j, \ldots w_n\}$ happening within the document where each w_j does not create adequate exposures to be measured precarious their combination achieved could be regarded as quasi-recognizers to be safeguarded. Here the concrete exposure created by PWs is the combination of separate exposures created by each w_j in terms of d_i estimated using Eq. (9.2). The medical record has to be cancer refined; the existence of the set of terms PWs = {urine blood level, cancer, tiredness} might be dangerous since the combination in immense correction with cancer through every discrete word creates an incomplete exposure [31].

To safeguard the mixture of precarious words, the autonomous and scattered storage produced by the multi-cloud by individually storing w_j or set of PWs is utilized. Likewise, the retarding of combined interfaces and eliminating the exposure the recollection of features of incomplete information is stored precisely [32]. The information segments shall be generated independently which satisfies the situations specified by the illustrations of the background refinement prototype after which they shall be stored individually to continue unpleasant to the service suppliers. It is also able to safeguard against unintentional disclosure by the service suppliers or peripheral attacks since they are incomplete data. The rest of the words within the documents that are not regarded as precarious shall be composed in an individual segment and stored in several cloud locations.

To rebuild the comprehensive document and to offer intelligible and comprehensive outcomes to the user-related requests, the proxy would store them on a local basis based on which there is metadata for each subcontracted document [32]. The list of words that are not subcontracted to the cloud are arranged separately because of their autonomous understanding they are organized based on their presence within the document. There is a list of cloud locations of the quasi-locating word PWs based on their balance within the information segments where they are held. The lists are organized based on the precedence of quasi—the location of words within the document.

The cloud location of the refined document is produced based on the elimination and location of quasi-located words. The positions they acquired within the document are labeled with custodian; likewise the proxy would be capable of rebuilding the document by simply substituting them with the elements in the locally organized list of locators and the subcontracted quasi-locators acquired from the precise service suppliers based on the locally organized list of cloud locations and their counterbalance to each location [32].

The key disputes of the subcontracting process are that the number of needed positions is also an immense number of positions; that is, an immense number of requests shall be accomplished to acquire the entire context for the document [33]. Two features have key effects on the needed positions. The depiction of the confidentiality prototypes allows arranging the interchange among the extent of safety and number of diverse cloud locations needed to satisfy the confidentiality assurances; that is, precisely the more the fixed values the severer is the safety along with the immense number of positions required to satisfy confidentiality conditions [17, 25, 32]. For larger documents, the exposures are constricted and the confidentiality prerequisites are severe as the number of quasi-locators that are stored individually might be huge. For minimizing the expenses and reducing the solution the intention is to design a desirous segmentation and distribution scheme which integrates diverse experiments to reduce the number of cloud positions *cPos* needed to store the documents which assures that each information segment satisfies the confidentiality prototypes [34]. The scheme intends to make use of several words w_j for every segment, s, where the combination still satisfies the confidentiality conditions and only when the condition is not satisfied a fresh segment is generated and the process is reiterated till no more is remaining to be distributed.

9.7.5 Data Segmentation and Scattered Storage

```
id // Input Document
PWs // Precarious Words
di // Arranged set of objects to be safeguarded
o(di) // Arranged a set of overviews related to di
id′ = id // id′ is the refined version of id
while ((not(null PWs))) do
    PWs = acquire delicate mixture (PWs)
    if (|PWs|==1) then
        substitute (PWs, id′)
        append (PWs, List_id)
    else
        substitute (PWs, id′)
        ic = acquire informative words (PWs)
        while ((not(null PWs)))
            position_located = false
            segment= initial (set of segments)
            while (not(position_located) && segment ≠ null)) do
                ws = segment + ic
                if(not(verifedexposure (di, o(di), ws))) then
                    position_located = true
                    append (segment, ic)
                    discard (ic, PWs)
                    ic = acquire rest of the words (PWs)
                else
                    segment = next (set of segments)
                endif
            end while
            if (not (position_located)) then
                if (|ic |==1) then
                    segment= fresh segment (ic)
                    append organized (segment, set of segments)
                    discard (ic, PWs)
                    ic = acquire rest of the words (PWs)
                else
                    PWs = acquire delicate mixture (PWs)
                endif
            endif
        end while
    endif
end while
for each segment in the set of segments do
    cPos=hoard individual cloud position (segments)
    append(cPos, list of cPos segments)
endfor
doc_cPos=hoard individual cloud position (id′)
hoard locally (id_cPos)
(organizeList_id, organize List_cPos) = acquire organized list

(List_id, set of segments, List_cPos, segments, id)
store metadata locally (organize List_id, organize List_cPos)
```

9.8 Performance Analysis

There are two features of the designed system which could be analyzed: the precision of the identified precarious words and the efficiency of the segmentation process. The results of the preceding are previously described and assessed which reveals that the execution of the background refinement with discreetly common fixed values accomplishes similar performance. The outcomes of the analysis and the efficiency of the segmentation process along with the designed schemes were recorded. The number of cloud positions with the quantity identical to the employed analysis on the document refinement has been carried out.

For analysis, a similar document quantity was employed to calculate the precision of the identification of precarious words. It holds a set of recitation documents entailing some objects that are delicate based on the prevailing legal contexts on the confidentiality of the information and extremely delicate individuals [35]. About the previous, the policies on the medical information confidentiality instruct hospitals and healthcare firms to safeguard the situations made to transmitted ailments for persistent medical documents before freeing them for instance insurance firms in reply to the employee reimbursement or motor automobile chance entitlement. These words openly mention that these are ailments and these are semantically associated with indications that shall be safeguarded. Similarly, the European Union Information Safety Instructions state that safety should evade probable discernment. For all these cases the feature exposure along with safety has to be offered. Wikipedia is employed based on the literature since they organize stimulating information safety conditions due to their snug and semantically opulent exposures [36] (Fig. 9.4).

To provide these sorts of information safety for every document, it is essential to make use of a diverse variety of illustrations of the background refinement framework. Initially, the basic HIV refinement is performed uniquely for the

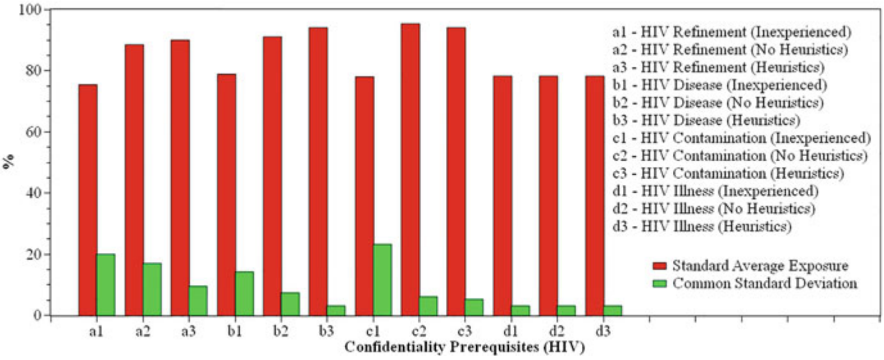

Fig. 9.4 Various confidentiality requisites for different heuristics schemes for the data collection of human immunodeficiency virus and its illness

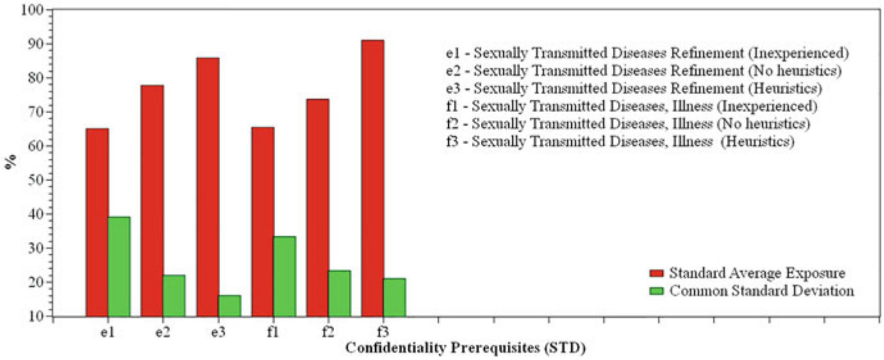

Fig. 9.5 Various confidentiality requisites for different heuristics schemes for the data collection of sexually transmitted disease and its illness

corresponding documents where the independent words or group of words that disclose the elements to be safeguarded are regarded as precarious. Following this semantically logical overviews are employed as fixed values to demonstrate the utmost extent of permitted exposures [37]. Disease, contamination, and illness were employed as overviews of HIV which is diagnosed as the sexually transmitted disease (Fig. 9.5). These case analyses are employed to demonstrate the mechanism of background refinement which could be naturally illustrated to the unit where the confidentiality statements are represented in the prevailing rules on information safety and for diverse confidentiality prerequisites.

9.8.1 Evaluation Parameters

To estimate the advantages designed based on the semantic information segmentation schemes the entailed segmentation policies are designed and used for the assessment. The inexperienced schemes for every delicate word are stored in a unique position. The comprehensive unfamiliar policies slightly satisfy the confidentiality prerequisites though it will probably need an immense number of positions. Routine 2 without the heuristics arranges the words and segments for increasing the unintended location of lawful provision [38]. Here the words are arranged identically as they are prevailing within the document and segments are assessed based on the conception. Scheme 2 based on the designed heuristics is entailed in data segmentation and scattered storage scheme. To estimate the efficiency of each segmentation policy, the below-entailed quality parameters are enumerated.

A number of cloud positions are required to assure that all the information segments are stored in precise format satisfying the confidentiality prerequisites [7, 15, 38, 39]. It is a vital feature that commonly states that with increased cloud positions immense is the expense of storage experienced by the users of the service suppliers. Furthermore more positions indicate more requests scattered for satisfying the input request and more outcomes shall be combined to offer comprehensive outcomes to the users. More positions are required to store the rest of the non-precarious words from the input document [8, 40, 41].

The exposure equalization among the cloud positions is estimated since the group of words is stored collectively based on the combined volume of data they expose where an improved distribution will be in combination exposed at every position where the closest exposure fixed value is entailed by the framework illustration [42]. Furthermore, the improved exposure-based equalization will be imitated based on a minimal difference among the extent of exposure of the words stored at every position; in the same manner identical extent of exposure is accomplished where several positions reveal meaningful data whereas others reveal crucially fewer data. Precisely, the heuristics method arranges the position of words to distribute the uniform equalization. To estimate the efficiency of the heuristics estimation of numerical average and the standard devotion of the combined exposure of the group of words stored in segments at every location has been recorded & analyzed. To provide numerals that could be straightforwardly estimated for diverse documents and framework illustrations normalization of every parameter based on the information exposure fixed value $o(d_i)$ is represented for the framework as below:

$$\text{normalized\_parameter} = \left(\frac{\text{parameter}}{d_i\ (\text{exposure\_fixed\_value})} \right) * 100 \tag{9.4}$$

Here the parameter relates to either the numerical average or the standard deviation of the combined exposure of the positions employed [43]. An improved and normalized average will be closer to 100% while an improved standard deviation will be 0%.

9.9 Results and Discussion

The assessment parameters for diverse documents, framework illustrations, segmentation processes, and heuristics employed are depicted in Tables 9.1, 9.2, 9.3, and 9.4. It is also depicted that these tables reveal the proportion of words from the entire document that were labeled as locators and quasi-locators.

Initially, it is perceived that the proportion of recognizing words escalates as per the refinement threshold. It is logical to fix common value, where the most common words are linked to the elements to be safeguarded could be missing words from data. An overview of the exposure threshold remains as locator that could not be stored precisely without negotiating the confidentiality prerequisites [44]. It is because of the requirement to locally hoard them within the proxies which guzzle

Table 9.1 Assessment parameters for the document regarding HIV with diverse segmentation policies and confidentiality prerequisites

Confidentiality prerequisite illustration	Locators (%)	Quasi-locators (%)	Segmentation policies	Standard average exposure (%)	Common standard deviation (%)
HIV refinement	6.5	15.0	Inexperienced	75.4	20.0
			No heuristics	88.5	16.89
			Heuristics based	90.01	9.52
HIV, disease refinement	9.8	13.5	Inexperienced	78.89	14.05
			No heuristics	90.99	7.23
			Heuristics based	94.00	3.02
HIV, contamination refinement	6.0	10.5	Inexperienced	78.02	23.23
			No heuristics	95.22	6.02
			Heuristics based	94.02	5.05
HIV, illness refinement	23.1	1.1	Inexperienced	78.21	2.99
			No heuristics	78.21	2.99
			Heuristics based	78.21	2.99

Table 9.2 Assessment parameters for the document regarding sexually transmitted diseases with diverse segmentation policies and confidentiality prerequisites

Confidentiality prerequisite illustration	Locators (%)	Quasi-locators (%)	Segmentation policies	Standard average exposure (%)	Common standard deviation (%)
Sexually transmitted disease refinement	5.5	10.2	Inexperienced	65.02	38.99
			No heuristics	77.75	22.0
			Heuristics based	85.85	16.02
Sexually transmitted disease, illness refinement	4.2	11.1	Inexperienced	65.4	33.3
			No heuristics	73.7	23.3
			Heuristics based	90.9	20.99

Table 9.3 Assessment parameters for the document regarding religions with diverse segmentation policies and confidentiality prerequisites

Confidentiality prerequisite illustration	Locators (%)	Quasi-locators (%)	Segmentation policies	Standard average exposure (%)	Common standard deviation (%)
Religion refinement	4.5	13.2	Inexperienced	76.75	25.55
			No heuristics	84.02	24.5
			Heuristics based	86.87	15.5
Religion, caste refinement	9.5	9.5	Inexperienced	79.00	21.1
			No heuristics	80.02	12.2
			Heuristics based	85.6	6.98

Table 9.4 Assessment parameters for the document regarding homosexuality with diverse segmentation policies and confidentiality prerequisites

Confidentiality prerequisite illustration	Locators (%)	Quasi-locators (%)	Segmentation policies	Standard average exposure (%)	Common standard deviation (%)
Homosexuality refinement	1.8	12.5	Inexperienced	62.98	50.98
			No heuristics	77.1	28.02
			Heuristics based	80.99	15.25
Homosexuality, illness) refinement	2.0	13.1	Inexperienced	63.23	39.98
			No heuristics	75.24	21.21
			Heuristics based	88.88	17.03

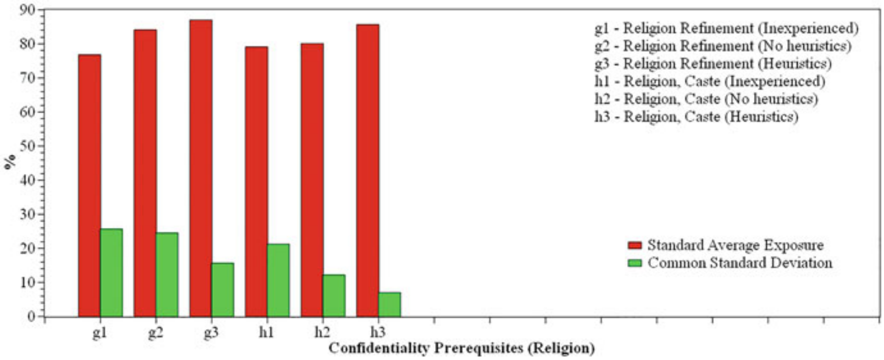

Fig. 9.6 Various confidentiality requisites for different heuristics schemes for the data collection of religion and caste

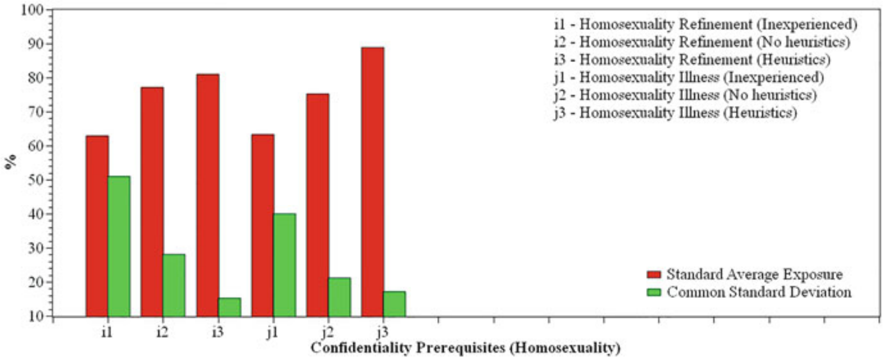

Fig. 9.7 Various confidentiality requisites for different heuristics schemes for the data collection of homosexuality and its illness

all the local storage supplies. Therefore it is perceived from the table that the locally stored locators experience minimal proportion of the overall volume of information to be subcontracted; furthermore it is crucial to recollect that these sort of documents are employed in worst-case conditions for information safety. It is also regarded as the number of positions required to store the quasi-locators for safeguarding confidentiality in a manner that it escalates the fixed values irrespective of the segmentation policies. The common fixed value entails increasing synchronization within the document which could expose in combination more data that could be entailed based on the fixed values (Figs. 9.6 and 9.7).

Therefore the firmest confidentiality conditions executed based on the common fixed value restrict the number of words stored together and escalate the number of required positions. The only exclusion is HIV documents (Fig. 9.4) for which many quasi-locators act as locators which could be employed for storing in one position but encoded form while creating a common fixed value. Based on the evaluation of diverse segmentation policies it is precise that the raw scheme offers the nastiest outcomes because it demands the principal number of positions [45]. Routing 2 crucially minimizes the number of required positions because it attempts to appropriate as many words as probable in each position till the confidentiality prerequisites are satisfied. The heuristics combined based on the routines also aids in enhancing the effectiveness of the distribution. Based on the arrangement of words in minimizing the demand for the information it attempts to assign initial words that execute the firmest limitations and will, therefore, be more intricate for distribution [46]. Based on the arrangement positions, the escalating demands of the combined exposures where the attempt is to make use of these segments has been more possible to fit a fresh word since there will be an exposure before negotiating the confidentiality prerequisites. It not only offers more effective employment of the prevailing resources but also minimizes the number of ineffective distribution tries in assessment based on the non-heuristic policy [47]. The heuristic scheme offers immensely related enhancements over the prevailing policies during the minimally firm confidentiality conditions mentioned, i.e., since no overviews are employed as exposure fixed values. Certainly, these configurations offer more extents of liberty to assign words without satisfying the confidentiality frameworks which the routines regard as merits.

The efficiency of the distribution process is demonstrated based on the equalization of exposure extents based on diverse positions employed. Based on the heuristics schemes the normalized average remains maximum and it is closer to 100% which represents that the exposure budget provided by every position in terms of fixed values is frequently used. Similarly, the standard deviation among the locations remains minimal which permits that the exposure extents of several positions are consistently equalized [47].

In the case of immobilizing the heuristics, the outcomes are somewhat inferior which much more gets inferior with the simple scheme. Here the distribution is nearly arbitrarily which means that the immense distribution budget is unexploited [48]. The outcomes are logical for all the documents irrespective of the confidentiality prerequisites inferring the private information like illness or recognition of information like name of the individuals [49, 50]. It is regarded that the heuristic-based segmentation policies briskly attempt to store the words which provide terminated data due to their synchronization which does not crucially escalate the levels of exposure of the segments while the split-balancing words with least shared data are stored independently.

9.10 Summary

Mostly the encoding serves as the key scheme for safeguarding confidentiality used to safeguard the subcontracted information over the cloud though it normally obstructs effectiveness both on the cloud and local sides for storage and location/recovery process which is not apparent for cloud suppliers which provide restricted services for the subcontracted features and append several problems like local managing of keys and the requirement to organize individually designed software components in the cloud to aid precisely subcontracted features. In comparison to the semantic-based information segmentation scheme, the intention is to design a curious alternate since all the subcontracted information is stored in precise form; the information organization is expandable and effective particularly during the location and revival process since it is fully translucent for cloud service suppliers that are not conscious about the information safety which preserves their services completely where the subcontracted features are directly safeguarded even for immense mobile exploration requests [14, 45].

Furthermore, the scheme creates a pre-planned confidentiality assurance provided by the background refinement framework which in contrast to estimation with other confidentiality frameworks is based on the algebraic and planned information which could be innately illustrated at an abstract level based on the semantic labeling. It permits the users to easily describe their confidentiality prerequisites without requiring them to be conscious of the procedures regarding information safety and also protects a unified implementation of prevailing semantics on qualitative information safety [48]. The framework permits describing the extent of safety made use of the information as a function of the volume of semantics that could be exposed. It is revealed that based on the simulation it also permits the equalization of the transaction among the extent of confidentiality and the volume of supplies required for implementing them.

Based on the comparison of the other safety schemes based on the information segmentation the essential semantic scheme for the designed approach makes it probable to mechanically estimate the threats prevailing on the safety of information based on the semantics they expose. It discharges the users from the liability of physically recognizing the delicate chunks of information as required based on the analysis and provides natural services for unplanned text-based information that could be barely organized by most of the prevailing confidentiality safeguarded solutions [27]. The intention is to design a semantic-based information segmentation that is capable of mechanically identifying information chunks that might create danger and divides them from the restricted principles so that every segment does not face any possible threats followed by which the segments of the flawless information are freely stored into individual positions of a multi-cloud, so no peripheral objects can gain access to the comprehensive private information. The forthcoming section portrays the conclusion of the designed works and future scopes.

9.11 Conclusion

With the aid of safe multiparty estimation, diverse individuals could estimate processes based on their input values without disclosing any data regarding their personnel input during the estimation. Here multiparty estimation is implemented among diverse clouds. By using safe multiparty estimation a better safety could be offered for the user's information for online-based services prevailing and employed nowadays but also has the perspective to perform fresh likelihood services which do not subsist currently due to the secrecy of user's prerequisites and lack of faithful third parties.

The forthcoming intention is to analyze the requirements for a standard confidentiality safeguarding prototype which intends in performing a choice in safeguarding the consumer's private information deposited into the cloud depository service suppliers. The growing improvements might cause the consumers of the cloud to miss their authority over the depositories. But the intention is to please the long-lasting distress of the consumer's prerequisite and the anticipated support and their precious information are of the system consumption which investigates the boundless support. The consumers of the cloud are forced to distribute their comprehensive facts and the data to the suppliers by tolerating the suppliers of the cloud tenure and provisions. It is noted that only up to 10% of the cloud consumers are conscious of the truth that the suppliers hold the entry to their private data. This becomes a significant problem in the rising cloud depository. The intention is to resolve the problems and to design a fresh common scheme with prototypes in safeguarding and maintaining the confidentiality of the consumers.

Though cloud computing offers several essential advantages such as cost cutdowns, accessibility, and expandability there arise issues related to the safety of information due to the missing of controls over the storage and administration of the outsourced information which still retards several users from transferring to the cloud environment. There is a diverse confidentiality safeguarding scheme based on the pre-planned encoding of outsourced information. The information encoding provides vigorous safety but the expenses in obstructing the effectiveness of the services and feature restrictions are employed over the encoded information onto the cloud environment. Since effectiveness and features are significant merits of cloud computing particularly in SaaS it is essential in designing a confidentiality safeguarding scheme that is dependent on dividing the information and based on the scattered storage provided by the progressively standard schemes of multi-clouds.

Precisely the intention is to design a semantic-based information segmentation that is capable of mechanically identifying information chunks that might create danger and divides them from the restricted principles so that every segment does not face any possible threats followed by which the segments of the flawless information are freely stored into individual positions of a multi-cloud so no peripheral objects can gain access to the comprehensive private information. It is to be noted that the fractional information is stored in vibrant cloud environments; the outsourced characteristics are effortlessly and effectively aided by distributing the requests to several cloud positions.

9.12 Future Scope

For imposing a vibrant safety concern the intention is to design a confidentiality prototype that provides a pre-planned confidentiality assurance for assuring its probability for which the proposal of empirical schemes reduces the number of cloud storage positions for depicting their abilities and precisely they are used for the least designed and most exciting information varieties. The future work is focused on enhancing the schemes, strategy, and authentication policies in active real-time cloud environments for adjusting its viability without completing the behavior of cloud computing.

References

1. Razaque A, Syed S (2017) Privacy-preserving model: a new scheme for auditing cloud stakeholders. J Cloud Comput Adv Syst Appl 6:7
2. Kang B, Wang J, Shao D (2017) Attack on privacy-preserving auditing schemes for cloud storage. J Math Probl Eng 2017:8062182
3. Bellare M (2003) Foundations of group signatures: formal definitions, simplified requirements, and a construction based on general assumptions. In: Advances in cryptology, pp 614–629
4. Blanton M (2008) Online subscriptions with anonymous access. In: Proceedings of symposium on information, computer and communications security. ACM, pp 217–227
5. Boneh D, Shacham H (2004) Group signatures with verifier-local revocation. In: Proceedings of the 11th ACM conference on computer and communications security, pp 168–177. https://doi.org/10.1145/1030083.1030106
6. Chadwick DW, Kaniz F (2012) A privacy-preserving authorization system for the cloud. J Comput Syst Sci 78:1359–1373
7. Yang C, Yu M, Hu F, Jiang Y, Li Y (2017) Utilizing cloud computing to address big geospatial data challenges. J Comput Environ Urban Syst 61:120–128
8. Chen Y, Sion R (2010) On securing untrusted clouds with cryptography. In: Proceedings of the 9th annual ACM workshop on privacy in the electronic society, pp 109–114
9. Sanchez D, Batet M (2016) Privacy-preserving data outsourcing in the cloud via semantic data splitting. Int J Comput Appl 10(2):1–26.
10. Malina L, Hajny J (2011) Accelerated modular arithmetic for low-performance devices. In: Proceedings of the 34th international conferences in telecommunications and signal processing. IEEE, pp 131–135
11. Mowbray M, Pearson S (2009) A client-based privacy manager for cloud computing. In: Proceedings of the fourth international ICST conference on communication system software and middleware, pp 5:1–5:8
12. Kaaniche N, Laurent M (2017) Data security and privacy preservation in cloud storage environments based on cryptographic mechanism. J Comput Commun 7(6):120–141.
13. Nguyen L, Safavi-Naini R (2004) Efficient and provably secure trapdoor-free group signature schemes from bilinear pairings. In: Journal of advances in cryptology, pp 372–386
14. Okamoto T, Uchiyama S (1998) A new public-key crypto system as secure as factoring. J Adv Cryptol 1403:308–318
15. Padma M, Geetharamani G (2018) Secured therapeutic applications for drug repositioning in the cloud computing. J Comput Life Sci Smart Technol Adv 29(1):65–68.

16. Raghavendra S, Girish S, Geeta CM, Rajkumar Buyya, Venugopal KR, Iyengar SS, Patnaik LM (2017) Split keyword fuzzy and synonym search over encrypted cloud data. J Multimedia Tools Appl 77(3):10135–10156.
17. Raja R (2017) Public key based third party auditing for privacy preservation in cloud environment. Int J Pure Appl Math 116(11):1–9
18. Nigam R, Chachapara K (2014) A survey on cloud computing. Int J Sci Eng Res 5(2):15–19.
19. RanjeetMasram VS, Abraham J, Moona R (2014) Analysis and comparison of symmetric key cryptographic algorithms based on various file features. Int J Netw Security Appl 6(4):43–52.
20. Sailaja K, Usharani M (2017) Cloud computing security issues, challenges and its solutions in financial sectors. Int J Adv Sci Technol Eng Manage Sci 3(1):190–196.
21. Mohite SP, Barve SS (2017) Encryption based cloud data search technique for privacy-preserving. Int J Comput Sci Inform Technol 8(3):330–334
22. Sumitra J (2013) Comparative analysis of AES and DES security algorithms. Int J Sci Res Publ 3(1):1–5.
23. More SS, Chaudhari SS (2016) Secure and efficient public auditing scheme for cloud storage. In: Proceedings of the international conference on computing, analytics and security trends. IEEE
24. Thillaiarasu N, Chenthur Pandian S (2016) Enforcing security and privacy over multi-cloud framework using assessment techniques. In: 2016 10th international conference on intelligent systems and control (ISCO), Coimbatore, pp 1–5. https://doi.org/10.1109/ISCO.2016.7727001
25. Shyamambika N, Thillaiarasu N (2016) A survey on acquiring integrity of shared data with effective user termination in the cloud. In: 2016 10th international conference on intelligent systems and control (ISCO), Coimbatore, pp 1–5. https://doi.org/10.1109/ISCO.2016.7726893
26. Thillaiarasu N, Susmitha M, Devadharshini D, Anantharaj T (2019) Solar powered fire extirpation robot with night vision camera. In: 5th international conference on advanced computing and communication systems (ICACCS), Coimbatore, India, pp 741–744. https://doi.org/10.1109/ICACCS.2019.8728438
27. Thillaiarasu N, ChenthurPandian S (2019) A novel scheme for safeguarding confidentiality in public clouds for service users of cloud computing. Cluster Comput 22:1179–1188. https://doi.org/10.1007/s10586-017-1178-8
28. Thillaiarasu N, Pandian SC, Vijayakumar V et al (2019) Designing trivial information relaying scheme for assuring safety in a mobile cloud computing environment. Wireless Netw. https://doi.org/10.1007/s11276-019-02113-4
29. Thillaiarasu N, Chenthur Pandian S, Naveen Balaji G, Benitha Shierly RM, Divya A, Divya Prabha G (2019) Enforcing confidentiality and authentication over public cloud using hybrid cryptosystems. In: International conference on intelligent data communication technologies and Internet of Things (ICICI) 2018. ICICI 2018. Lecture notes on data engineering and communications technologies, vol 26. Springer, Cham. https://doi.org/10.1007/978-3-030-03146-6_175
30. Ranjithkumar S, Thillaiarasu N (2015) A survey of secure routing protocols of the mobile ad-hoc network. SSRG Int J Comput Sci Eng 2:1–7.
31. Swathi V, Vani MP (2017) Security and privacy challenges in cloud: survey and research directions. Int J Comput Eng Res 7(8):63–72.
32. Dilip TV, Dhake AR (July 2017) Privacy preserving in authentication protocol for shared authority based cloud computing. Int Res J Eng Technol 4(7):1108–1112.
33. Veeramachaneni VK (2015) Security issues and countermeasures in cloud computing environment. Int J Eng Sci Innov Technol 4(5):82–93.
34. Krishnan V, Hanumesh H, Nayak PD, Krishnamurthy MS (2016) OTP authenticated and encryption on cloud data. SEA Int J Adv Res Eng 1(1):1–4.
35. Lu W, Varna AL, Wu M (2014) Confidentiality preserving image search: a comparative study between homomorphic encryption and distance preserving randomization. J Transl Curr Mining 2:125–141.
36. Xue Y, Yin F, Tang X (2017) A fine-grained and privacy-preserving query scheme for fog computing—enhanced location-based services. Sensor J 17:1–14.

37. Wang Y, Zhang P (2017) Enhance big data security in cloud using access control. In: Proceedings of the international conference on advances in big data analytics
38. Zou D, Xiang P, Min G (2016) Privacy preserving in cloud computing environment. J Secur Commun Netw 9:2752–2753
39. Kim H, Ben-Othman J A virtual emotion detection system with maximum cumulative accuracy in two-way enabled multi-domain IoT environment. IEEE Commun Lett. https://doi.org/10.1109/LCOMM.2021.3060737
40. IEEE Smart Grid Vision for Computing: 2030 and Beyond Roadmap (2016) In: IEEE smart grid vision for computing: 2030 and beyond roadmap, pp 1–14
41. Albataineh H, Nijim M, Bollampall D (2020) The design of a novel smart home control system using smart grid based on edge and cloud computing. In: 2020 IEEE 8th international conference on smart energy grid engineering (SEGE), Oshawa, ON, Canada, pp 88–91. https://doi.org/10.1109/SEGE49949.2020.9181961
42. Sirojan T, Lu S, Phung BT, Ambikairajah E (2019) Embedded edge computing for real-time smart meter data analytics. In: 2019 International conference on smart energy systems and technologies (SEST), Porto, Portugal, pp 1–5. https://doi.org/10.1109/SEST.2019.8849012
43. Nkenyereye L, Hwang J, Pham Q-V, Song J MEIX: evolving multi-access edge computing for industrial Internet-of-Things Services. In: IEEE network. https://doi.org/10.1109/MNET.011.2000674
44. Guan Z, Zhou X, Liu P, Wu L, Yang W A blockchain-based dual side privacy-preserving multiparty computation scheme for edge enabled smart grid. IEEE Internet of Things J. https://doi.org/10.1109/JIOT.2021.3061107
45. Jamil F, Iqbal N, Imran SA, Kim D Peer-to-peer energy trading mechanism based on blockchain and machine learning for sustainable electrical power supply in smart grid. IEEE Access. https://doi.org/10.1109/ACCESS.2021.3060457
46. Yahuza M, Idris MYI, Wahab AWBA, Nandy T, Ahmedy IB, Ramli R An edge assisted secure lightweight authentication technique for safe communication on the internet of drones network. IEEE Access. https://doi.org/10.1109/ACCESS.2021.3060420
47. Shang M, Yuan Y, Luo X, Zhou M An α-β-divergence-generalized recommender for highly accurate predictions of missing user preferences. IEEE Trans Cybernet. https://doi.org/10.1109/TCYB.2020.3026425
48. Chen R, Wang X, Liu X Smart futures based resource trading and coalition formation for real-time mobile data processing. IEEE Trans Serv Comput. https://doi.org/10.1109/TSC.2021.3060343
49. Al-Obaidi AA, Farag HEZ Decentralized quality of service based system for energy trading among electric vehicles. IEEE Trans Intell Transport Syst. https://doi.org/10.1109/TITS.2021.3058514
50. Tiwary P, Pandey A, Kumar S (2021) Differential d-vectors for RSS based localization in dynamic IoT networks. In: 2021 international conference on COMmunication systems & NETworkS (COMSNETS), Bangalore, India, pp 82–85. https://doi.org/10.1109/COMSNETS51098.2021.9352896