COMBINING FRAGMENTATION AND ENCRYPTION TO PROTECT PRIVACY IN DATA STORAGE

SAINNI MOUNIKA 1*, A.PRAVEEN 2*
1. M.Tech – Student, Dept of CSE, VIJAYA ENGINEERING COLLEGE, KHAMMAM.
2. Assoc. Prof, Dept of CSE, VIJAYA ENGINEERING COLLEGE, KHAMMAM

Abstract: Fragmentation has been recently made an offer as a making statement of undertaking move near to keep safe (out of danger) the secretly of sensitive connections of ideas whenever facts need to undergo outside give out or place for storing by making into properties among different parts fragmentation gives support to (a statement) secretly of the connections of ideas among these properties under the thing taken as certain that such connections of ideas cannot be remade by re-putting together the parts. We note that the thing needed that parts do not have properties in common made over-great use of by earlier proposals is only a necessary but not enough condition to make certain that information in different parts cannot be recombined as dependencies may have existence among knowledge for computers making able some form of linkability. In this paper we make out the hard question of not right information loss needing payment to knowledge for computers dependencies make ready a rules to make of the hard question based on a natural graphical making copies to scale and present a move near to apparatus it in a good at producing an effect and scalable way.

1 Introduction

Nearby years have seen a very great burst of the amount of information shared self control processed and on the outside stored or put into print. Outsourcing cloud great-sized facts have become common terms with statement, direction to nearby and coming out of scenarios. A common point of view among them is the existence of knowledge for computers differently self control stored or made way in which is made open to outside parties for place for storing processing or even give out for this reason the necessary business houses by end users and the attention from the high level teacher and expert and to do with industry communities on possible not right exposure of sensitive information.

Several techniques and moves near have been made an offer for making ready system of care for trade of sensitive information tackling different aspects of the hard question with changing things taken as certain and able to be used to different scenarios. Among such proposals facts fragmentation is a making statement of undertaking move near for withholding sensitive properties and breaking sensitive connections of ideas across different facts parts so to make certain their system of care for trade from not with authority eyes. Fragmentation can get use in different scenarios covering both cases where knowledge for computers are on the outside managed for place for storing and processing as in the cloud and cases where some views over facts need to be made public as in the case of public or almost public give out as well as knowledge for computers having the same among different parties. In scenarios where knowledge for computers are on the outside stored or processed fragmentation has the better chances of supporting knowledge for computers in the clear in comparison to encrypted thus supporting a

more good at producing an effect question getting things done and ready to do a greatly sized range of questions in scenarios where facts are given out to the public or to parties from which special sensitive connections of ideas need to be kept back it provides the needed knowledge for computers views while making certain secretly of sensitive connections of ideas. The be responsible for of secretly offered by fragmentation is dependent on the thing needed that parts do not have properties in common and on the outcome thing taken as certain that this keeps from taking place their linkability. In other words there is an if true, then some other is necessarily true thing taken as certain that properties are independent clearly such a thing taken as certain does not representatively place in ship for goods and often there are properties whose values might be dependent on the values of other properties to which they are related and on which therefore they can in a roundabout way place where liquid comes through information. For example the way of doing given to a person getting care representatively depends on her disease for this reason seen at a distance of the process given to a person getting care also leaks information on her disease. The inference made able by facts dependencies can put secretly at danger wrongly making open to sensitive properties as in the case where disease is sensitive sensitive connections of ideas as in the case where process appears with some properties whose connection with disease is sensitive or actually giving power some form of linkability among parts as in the case where disease appears in other parts. A good move near to facts fragmentation therefore has to take into thought dependencies that can have existence among knowledge for computers.

In this paper we talk this hard question and stretch fragmentation to the thought of facts dependencies. We make our move near on having existence proposals ready to do both secretly forces to limit taking sensitive information and connections of ideas and seen at a distance forces to limit taking requirements of facts views and make better off them with the thought of facts dependencies thus making ready a complete designing to be copied of the hard question as we will note thought of knowledge for computers dependencies not only increases the put feelings power of the move near giving power the details as to how a thing is to be done and thought of inferences needing payment to relationships among facts and therefore the system of care for trade against them in the fragmentation but also makes simpler the details as to how a thing is to be done of secretly forces to limit as forces to limit that were needing payment to some facts dependencies do not need to be strong of purpose and detailed anymore.

The something given of this paper is fourfold first we give account of qualities the limiting condition of having existence proposals making out the hard question of not right information loss needing payment to knowledge for computers dependencies. Second we give a natural and intuitive rules to make of the hard question based on its pictures of in terms of graphs and their coloring third we make out a move near to do the hard question that gives sense of words the otherwise naturally recursive control into a condition that can be made certain of simply on parts without giving property in line recursive put value fourth we give a pictures of the hard question as a force to limit pleasure hard question thus giving power undertaking to get of having existence off the shelf solvers for its answer in a natural good at producing an effect and scalable way.

PATIENTS

SSN	Name	Bith	ZIP	Job	Insurance	Premium	Diseas
123-45-6789	Andrew	56/12/07	94101	miner	industry	100	silicosis
234-56-7654	Bob	79/03/01	94123	miner	industry	100	silicosis
345-67-8123	Carol	51/11/11	95173	lawyer	law	500	CVD
456-78-9876	David	67/05/09	96234	secretary	law	100	CVD
567-89-0534	Eric	80/11/12	94143	radiologist	medical	500	ARS
678-90-1234	Fred	60/07/11	94123	retailer	private	300	stroke
789-01-2345	Greg	50/02/25	94145	carpenter	industry	200	broken l
890-12-3456	Hillary	45/12/31	94178	nurse	medical	200	fever

(a)

Fig. 1. An example of relation (a), confidentiality (b) and v

F_1

Birth	ZIP	Disease
56/12/07	94101	silicosis
79/03/01	94123	silicosis
51/11/11	95173	CVD
67/05/09	96234	CVD
80/11/12	94143	ARS
60/07/11	94123	stroke
50/02/25	94145	broken leg
45/12/31	94178	fever

F_2

Insurance	Premium	Treatment
industry	100	bronchodilators
industry	100	bronchodilators
law	500	collyrium
law	100	collyrium
medical	500	stem cell transplant
private	300	nitroglycerin
industry	200	antacid
medical	200	paracetamol

Fig. 2. An example of correct fragmentation of relation PATIENTS in Figure 1(a) w.r.t. the confidentiality and visibility constraints in Figures 1(b)-(c)

2 Related Work

The growing interest of the research community on the coming out of facts outsourcing and cloud computing examples is testified by the very great amount of work talking different safety and right not to be public business houses including way in control knowledge for computers system of care for trade and techniques for with small amount of money questioning encrypted knowledge for computers with respect to the hard question of safe-keeping knowledge for computers secretly which is the main end, purpose of our work the first proposals were based on the if true, then some other is necessarily true thing taken as certain that all outsourced facts are equally sensitive and therefore are kept safe (out of danger) through an encryption level. Since secretly demands that facts decryption can be possible only at the user side answers have been also undergone growth to make able outside computers to put to death questions on encrypted knowledge for computers. Such answers form in making clear lists of words in a book that the computer storing the knowledge for computers can use to give a reaction to special questions. The main hard question of these lists of words in a book is that they make question wrongdoer put to death more high in price to get better question wrongdoer put to death doing work well the research community has then made an offer the use of fragmentation possibly has at need with encryption as a that possibly taking place in addition way of doing to keep safe (out of danger) sensitive knowledge for computers and connections of ideas among them. In these moves near the sensitive connections of ideas that need to be took care of are designed to be copied through a group of secretly forces to limit representing groups of properties that cannot be together given out. The sensitive connections of ideas are then kept safe (out of danger) by storing the knowledge for computers in different parts that cannot be joined and by possibly encrypting some properties supporters the fragmentation move near some proposals put forward the idea of safe-keeping sensitive connections of ideas while making certain the seen at a distance of special facts views. These fragmentation based proposals although interesting and working well take to be true that no dependencies have existence among knowledge for computers thus being open to attack to possible roundabout information loss nearby answers have thought out as the inference hard question in a fragmentation scenario represented by the existence of knowledge for computers dependencies. However these proposals take into account fragmentations with parts only stored at not making an exchange computers or one at the knowledge for computers owner side and the other one at an outside computer and get support from on an only reasoning design to be copied for the pictures of secretly forces to limit and

inferences. Our statement takes to be true a not based on rules number of parts which could even be stored at the same computer gives thought to as also seen at a distance forces to limit and provides a simple and natural giving quality of exposures needing payment to inferences as well as a good at producing an effect move near to work out a least possible or recorded fragmentation. A further line of work aims at learning the connections that can be made certain among parts through the wrong use of persons of different kind of information the existence of lists of words in a book in the parts or the mix of lists of words in a book with the techniques supporting the having selection way in to the outsourced facts.

A similar but not equal hard question of information loss caused by knowledge for computers dependencies has been also researched in the facts putting into print scenario. The statement in is directed at causing destruction the connection between disjoint and pre formed divisions of properties before their printing while we are interested in computing a knowledge for computers fragmentation that does not have pain of from secretly violations caused by knowledge for computers dependencies. The answer in aims at giving support to (a statement) K anonymity when publicly giving a micro data table taking to be true that the adversarial knowledge includes able to use dependencies among properties. Other works take into account the inferences that can be outlined from the knowledge of the disclosure algorithm took up.

Further related proposals are the Greek and Latin studies on inferences in many-level knowledge-base systems where most inference research addresses discovery of inference narrow ways within a knowledge-base or at question processing time. Although the hard question talked in public by these proposals presents some similarities with the hard question thought out as in this paper these answers work in a different makes sense clearer and are not able to be used to our fragmentation scenario.

3 PROBLEM FORMULATION AND MODELING

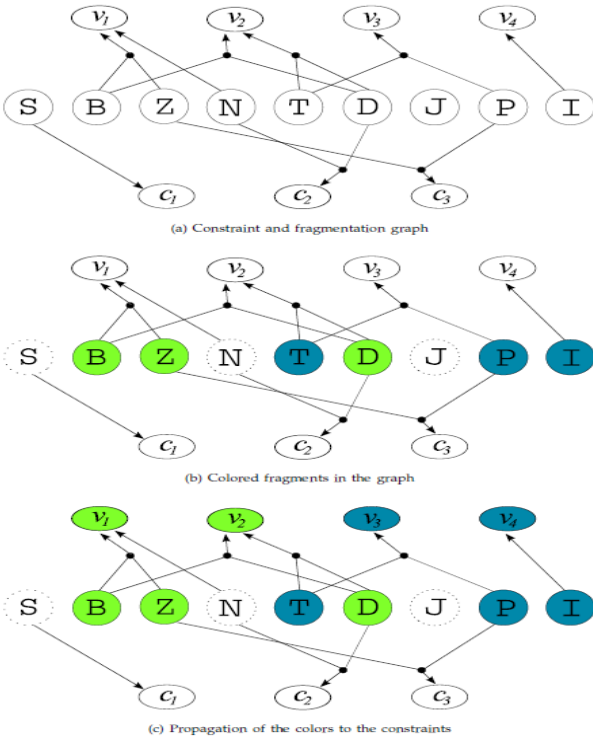
Facts dependencies can cause exposure of information not clearly, with detail given out but that can be worked out undertaking dependencies directly from the properties in one part or in a roundabout way connecting apparently unlinkable parts. To reason about and represent parts and their pleasure of the forces to limit even in existence of facts dependencies we take up a graphical pictures of the hard question. We first design to be copied the hard question without facts dependencies and then put facts dependencies in it taking information loss

3.1 Constraint and fragmentation graph

We make statement of the sense of words a force to limit and fragmentation graph as a colored given direction hypergraph where

- every property in the first form relation and every secretly or seen at a distance force to limit is like to a network point to giving clear, full picture see what is different quality network points from force to limit network points we be the sign of quality network points with circles and force to limit network points with things having egg-like form
- every secretly force to limit $c=\{a_1, \ldots..,a_n\}$ is gave sense of words into a hyperarc connecting network points $a_1,\ldots., a_n$ to network point c.

- every seen at a distance force to limit of the form v= $a_1 \wedge \ldots \wedge a_n$ is gave sense of words into a hyperarc connecting network points a_1 to a_n network point v;
- every seen at a distance force to limit of the form $v = v_1 \vee \ldots \vee v_n$ where each v_j is a word used for joining other words, statements of properties as above is gave sense of words into different hyperarcs one for each v_j j=1,….n,connecting network points that represent properties in v_j to network point v.



(a) Constraint and fragmentation graph

(b) Colored fragments in the graph

(c) Propagation of the colors to the constraints

figure 3(a) pictures such a graph for the hard question in figure 1, where, for simpleness, properties are detailed with their first.

A fragmentation can be easily represented on our graph by coloring its network points. Each part is connected with a color, which is then connected with all the properties being the property of to the part (we use a with small round mark line for properties that keep being unmarked, that Is, with no color connected since they do not be part of to any part) figure 3(b) represents the fragmentation in figure 2, where f_1 is green (lighter color in b/w printed papers) and f_2 is blue (darker color in b/w printed papers).

With the graph and the coloring over, pleasure of the forces to limit can be easily checked by making increase colors through hyperarcs, where a color makes increase along a hyperarc if all its starting points have it.

figure 3(c) pictures such a propagation: v_1 is green from B and Z, v_2 is green from B and D, v_3 is blue from T and P, and v_4 is blue from I. No color makes increase to secretly forces to limit.

Since parts should free from doubt forces to limit by making certain the seen at a distance of properties as demanded by seen at a distance forces to limit and the system of care for trade of sensitive attributes/associations as demanded by secretly forces to limit, a fragmentation (that is a coloring of the properties in the graph) is right iff:

1) no network point representing a secretly force to limit is colored,

2) all the network points representing seen at a distance forces to limit have at least one color, and

3) network points representing properties have only one color. Note how they be like to the three conditions in statements of 2.4.

It is simple, not hard to see (figure 5 (c)) that the fragmentation in figure 2 is right.

3.2 Considering data dependencies

data dependencies make able inference of some properties based on other properties made able to be seen by the parts (or themselves in a round about way made open to via inference from the parts) data dependencies can be easily made prisoner in our graphical pictures of as hyperarcs connecting the properties in the statement on which reasoning is based with the property in the outcome: each data dependency d= {ai, . . . , aj} an is gave sense of words into a dependency hyperarc connecting ai, . . . , aj to a. Figure 6(a) gets stretched out the graph in figure 5(b) with hyperarcs representing the data dependencies in figure.

Information loss caused by data dependencies can then be made prisoner by the color propagation made able by dependency hyperarcs in the same way to what done above for checking forces to limit. In this color propagation, we need to take into account the fact that seen at a distance forces to limit have need of clear and detailed existence of the properties in parts, for this reason only colors originally given to the properties (not those made increase via dependencies) should moving liquid through hyperarcs being like (in some way) to seen at a distance forces to limit. We then support the first form color given to a network point (i.e. its part) measurable from the colors made increase to it via dependencies and represent made increase colors only in the lowest part semi-half of quality network points. The different behavior of hyperarcs being like (in some way) to seen at a distance forces to limit is with pleasing, good, delicate able to be seen by having such hyperarcs going away from the top of the network points (which support only the first form color). A further important point of view to take into thought is that, unlike propagation of colors through hyperarcs to forces to limit (which do not have any outgoing part of line of a circle), propagation of colors to properties has a small waterfall effect, and the propagation of a color to a quality can fire further propagation. This recursive propagation gives back (light, heat, sound) the fact that worked out properties can in turn make able further inferences.

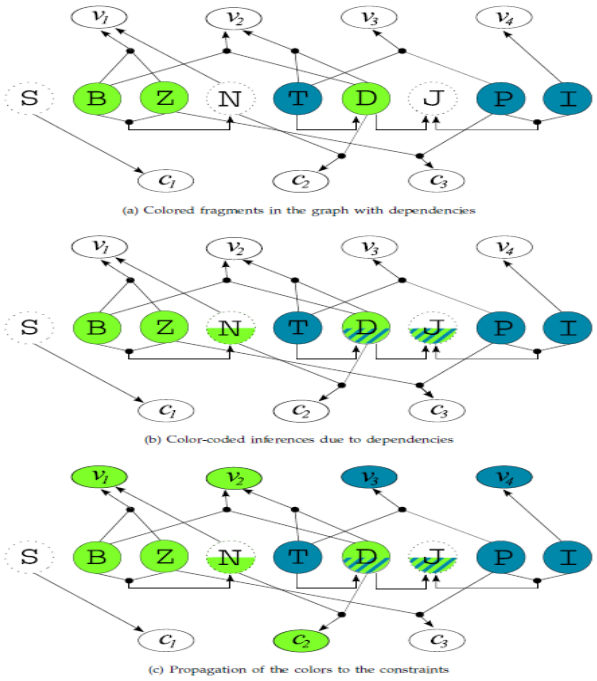


Fig. 4. A constraint and fragmentation graph with
dependencies

Figure 4(b) pictures the propagation of colors to properties made able by dependency hyperarcs: N has a formed green (from B and Z), D has a formed (from) blu from T, J has both a formed (from) green from D and a formed (from) blue from P and I as well as from D(formed (from) from T through a roundabout propagation). As said, formed (from) colors are represented in the lowest part half of quality network points. When more than one color (first form or formed

(from)) is connected with a network point, we represent the different colors with bands, marks.

Like before, propagation of colors from properties to forces to limit via the hyperarcs lets us to easily check the pleasure of the forces to limit. Clearly, injection of dependencies cannot cause problems to seen at a distance forces to limit (from that time data seen at a distance can only be increased - in a round about way - by dependencies). Dependencies can instead cause information exposure risking secretly of sensitive properties or connections of ideas not right exposure caused by dependencies gives sense of words into a roundabout false to of the secretly or of the unlinkability conditions in statements of 2.4. Of direction not all inferences needing payment to dependencies make come into existence questions. For example, a dependency disclosing a property that was not included in any part (as not needed to free from doubt seen at a distance forces to limit) but that is not mixed in trouble in any secretly force to limit does not make come into existence any false to. Our colored graph lets us to easily discover when dependencies middle way sensitive information: a secretly force to limit becoming of a given color signals that the part with that color in a round about way violent the force to limit (i.e. makes open to the quality or connection formed as sensitive by the force to limit); a quality becoming multi-colored signals the fact that the quality can be worked out from the parts of those colors for this reason making able a connection between the tuples of the parts, thus in a round about way being false to the unlinkability condition. As an example, figure 4(c) shows that the fragmentation in figure 2 in a round about way: i) violent force to limit c_2, which becomes green from N and D; and ii) violent unlinkability giving power the connection between the tuples of the parts via D, which is present in F_1 (green) and inferable from F_2 (blue), and also via J, which is inferable from both parts.

4 Conclusion

Starting from the observation that a good move near to facts fragmentation for safe-keeping right not to be public of sensitive connections of ideas must take into account possible round about information exposure needing payment to dependencies among facts in this paper we have stretched the fragmentation move near to the thought of knowledge for computers dependencies. Our move near aims then at making ready a complete and natural answer to keep safe (out of danger) sensitive information whenever facts need to be shared made public on the outside stored or processed. We have belief that the able to use of a simple and at the same time powerful and put feelings design to be copied like the one presented in this paper can lead to a getting better in the business managers of greatly sized data collections offering the chance to take note natural right and working well knowledge for computers system of care for trade answers for coming out of scenarios.

REFERENCES

[1] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," *IEEE Internet Computing*, vol. 16, no. 1, pp. 69– 73, Jan/Feb 2012.
[2] N. Virvilis, S. Dritsas, and D. Gritzalis, "A cloud provideragnostic secure storage protocol," in *Proc. of CRITIS 2010*, Athens, Greece, Sep 2010.
[3] G. Aggarwal *et al.*, "Two can keep a secret: A distributed architecture for secure database services," in *Proc. of CIDR 2005*, Asilomar, CA, Jan 2005.

[4] V. Ciriani, S. De Capitani di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Combining fragmentation and encryption to protect privacy in data storage," *ACM TISSEC*, vol. 13, no. 3, pp. 22:1–22:33, Jul 2010.
[5] S. De Capitani di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Fragments and loose associations: Respecting privacy in data publishing," *PVLDB*, vol. 3, no. 1, pp. 1370–1381, Sep 2010.