4th International Conference on Current Research in Engineering Science and Technology (ICCREST-2019), Jayaram College of Engineering & Technology, Trichy, India.

CCA: A Methodical Vendee Vendor Carbon Copy Algorithm for Data Trading

M. Ayisha Siddhiqua [1], T. Arivulagarasi [2], M. Kanmani [3] ,V. Lakshmi [4] , B.Ezhilarasi [5]

[1234]Students, Department of Computer Science and Engineering, K.Ramakrishnan College of Engineering, Trichy

[5]Assistant Professor, Department of Computer Science and Engineering, K.Ramakrishnan College of Engineering, Trichy

[1]greatpebble@gmail.com

[2] arasi19797@gmail.com

[3] manimegalaikanmani@gmail.com

[4] suryavaradarajan98@gmail.com

[5] ezhilarasirani22@gmail.com

Abstract

Owing to the meteoric growth of Internet and cyberspace technology, digital data (images, audios, videos and datasets) can be seized easily. On one hand, this helps people to share digital merchandise with others. Contrarily illegal copies are produced and distributed with little efforts. To deter piratism and protect the proprietorship of digital products, digital carbon copy technology is introduced. A carbon copy is an imperceptible copy of the digital data maintained before selling, which can be detected later for vendee/vendor identification, ownership proof, traitor tracing and so forth. Vendee vendor carbon copy algorithm is designed to hinder clients from unjustly distributing copies of digital content. In this paper, an anonymous and interactive Carbon Copy Algorithm (CCA) is proffered, which is designed to be impartial and efficient. To solve the unbinding problem and the vendees' right problem, operations of carbon copy generation and digital content selling are performed by a Trusted Third Party in the proposed scheme. Vendees and vendors have equal rights and responsibilities, and computational and corresponding overhead is lessened. We show that the proposed protocol is highly accurate, secure and efficient.

Keywords: ***Proprietorship protection, unbinding problem, vendees' right problem, traitor tracing***

I. INTRODUCTION

The expeditious trading of digital merchandise has been elevated. This paradigm of dataset distribution has become a remarkable candidate for the business aeon. However the benefits of digital information exchange comes with increased security burdens. An issue concerning the proprietorship assurance arises regarding these digital datasets. Concerns may emerge with respect to modification and the owners of these data products. Due to the intangible nature of datasets, concerns may emanate when brokers may illicitly resell the datasets without the authorization of the concerned proprietor. Besides the aforementioned issue, risks of perturbation of these purchased datasets may arise and the brokers may deceitfully claim that they are the legal owners. A unique vendee-vendor carbon copy algorithm has been proposed to track down the illicit distribution of these dataset replicas and guarantee the proprietorship rights of the lawful owners. Content creators are ensured with indemnification of their original content and unlawful reselling can be averted. Taking into account the previously narrated issues, this paper includes plagiarism detection of the concerned digital datasets. The principal intention behind this is to make solely mandatory comparisons according to the semantics of the datasets. Semantically corresponding datasets are compared to recognize the potentially indistinguishable regions.

Further the plagiarized content under inspection is exposed by comparison of the datasets with the available datasets reserved within the extant database. High profile dataset breaches have content owners on red alert for safeguarding their data both now and for the future. Encryption which is a crucial asset in the security chain is done to block traitors from accessing the datasets involved in purchase. It aims in shielding the digital content against vulnerability exploits. Here time specific encryption is performed in order to heighten the efficiency. The content creator can stipulate a time interval amid the process of encryption and the vendee must decrypt to recover the dataset only within the corresponding time interval. The main eminence of our proposed approach is the capability of the trusted third party to perform verification of the datasets on behalf of the content owners and ensure the accountability by supervising the plenary process of encryption and decryption.

Since this scheme is based on a trusted third party, the proprietorship verification and other computations are well justified in our proposed strategy. Time harmonized one time passwords are involved in validating a genuine vendee. This approach provides a greater level of validation guarantee. Since it is true only during the stipulated time. Further the vendee can also trust that the purchased datasets cannot be accessed easily by any other anonymous persons. It also avoids the inconvenience of remembering the constant prefixed passwords. Another notable constituent involved in our proposition is session timeout which is a security and dataset management feature that automatically logs the vendee off the operation. Once the session expires, the dataset associated with the session is destroyed after the particular configured amount of time. The session is dynamically assigned and this setting applies, based on the content magnitude of the datasets. Finally our proposed schema should impose imperceptible overhead and must be practically acceptable to the consumers.

II. RELATED WORKS

Several propositions have been suggested for elevating the level of invulnerability in the interim of dataset trading. S.Brin et al., [1] presented a technique to uncover transcribed digital documents and counter the issue of copyright infringement. An entity for recording the digital content and reporting replicas was composed. A functioning paradigm labelled COPS which is a transcript disclosure service and a metric for replica detection was used. The service not only exposed transcriptions but also discovered overlapping documents. M.Felici et al., [2] introduced a theoretical prototype to achieve liability in the cloud framework. Accountability contributes a factor for fulfilling amenability analogous to administrative regimes ensuring confidentiality and security of data. This facilitates users to take responsibility for data maintenance and adhere to managerial commands. As a result cloud environments align themselves according to the rules to achieve a convincing cloud. In a cloud environment, awareness on responsibility for data control was created.

T.Truderung et al., [3] hinted that numerous tasks correlated with security and diverse operations comprising of immense number of persons are supervised by a reliable arbitrator or a third party. So it is pivotal that such mediators are culpable in any situation of insubordination or impropriety. In order to endeavour an authentic and plausible interpretation of accountability, figurative and estimational prototypes were suggested. According to the author, verifiability is affiliated with liability. L.Zhang et al., [4] propounded that due to the propagation of cellular phones, image sharing and service seeking has become more frequent. Owing to this, there is a high risk regarding the exposure of such personal photos and privacy leakage. Hence a protocol named POP was recommended to assure secure photo exchange and retain confidentiality. Individuals pursuing confidentiality concerning their private data were able to adopt to the suggested schema in order to only permit legal persons associated with the individual to browse and view their images. All modules involved in the paradigm allowed users to characterize exclusive content. However statistics in the suggested schema indicated a slight rise in overhead.

A.Z. Broder [5] developed a mechanism for determining the analogy of scripts in which the similitude with a steady amount of example for every script was assessed. Examination method was energetically applied with two processes such as resemblance and containment. Containment appraisal of little ones into the bigger is vulnerable to flaws due to the scarcity of scripts. Dactylograms are estimated to count the occurrences. Multiple insertions are evaded by keeping a binary search tree. The amount of example needs to be larger to get the most precise outcomes. X.Cao et al., [6] proposed a method to assign a sample size of data to miscellaneous users. For adept allocation of data by proprietors and to harmonize data trading, a well cultured auction mechanism was developed. The proposed method made the proprietors to trade properly and evaded the easy retrieval of owner's confidential details. Convinced properties are distinctive rationality and weakly equitable cost. Hence narcissistic proprietors who wish to improve their own services were evaded.

Y.Xiao [7] indicated that any paradigm must be answerable for its own particular demeanour or deed such that the paradigm is involved in bigger progressions of accountability. The prime objective of liability is that whenever a process has occurred and taken place, the segments that transpired are trackable such that the disputes can be resolved later. The faulty liability uncovered by current processors, squanders a mass volume of capital and effort. In order to conquer this, a peculiar technique called flow-net for accountability was proffered. A unique technique for traffic data compilation that can be used for exposure of malicious hackers as well as in forensics was schemed. L.Zhang et al., [8] implied that a burdensome issue in social media related applications is to safeguard the confidentiality of individuals and their personal data as these networks were introduced to aid intercommunication among users and guide persons to discover other individuals with an equivalent profile within a particular gap. In order to overcome the aforementioned concern, an innovative schema was proposed. Whenever a desired profile was requested by an individual, the search associated with the coordinating profile assured privacy conservation. The proposed technique guaranteed a secure connection medium between the users when the matching individual is spotted. The

schema was premeditated to be proficient as well as secure.

S. Delgado-Segura et al., [9] proffered a procedure for performing data trading in an efficient manner. The Bitcoin scripting language was used in designing the procedure. The main aim of the project was to avert the doubtfulness among the traders in financial transactions. So, the protocol was developed in such a way to eliminate the favourable situation to neither of the traders. Private keys with bitcoins were used in the transaction. As a result every transaction was either completed successfully or none of the traders were affected by that transaction in data trading. X-Y. Li et al., [10] devised a scheme for safeguarding the confidential data dissemination with the help of a graph which conceals the hereditary pertinence linking of data into a graph format notably. They developed an innovative graphical depiction suitable for all kinds of datasets and also a spectrum graph separation algorithm to build graphs corresponding to various forms of datasets. They also decided certain measures to determine the accuracy of scheme from other unknown methods. The scheme was finally strong enough to compute anonymous security risks under different situations.

III. CCA: A PROPOSED TECHNIQUE

Our specified protocol is comprehended with the subsequent participants. These parties must be liable for their trading related activities. They are listed as follows:

Vendor:

Vendors need to load only their unique datasets for which they hold proprietorship rights. They must refrain from unlawful reselling of pirated datasets and if they deteriorate from their duties, it is referred to as misconduct.

Vendee:

Vendees are strictly directed to purchase the loaded datasets with the aid of the authentication center. They are solicited to thwart any kind of manipulation or act as a broker. They are expected to only view the datasets, within the designated session time.

Authentication center:

The overall data trading process is monitored and authenticated by this trusted center. The center is responsible for detecting fraud replicas and acquainting the participants in case of any insubordination.

The following steps elaborate the proposed CCA algorithm as follows:

Step 1: The vendor (V), who wants to make a financial gain on the sales of certain digital content he owns may be the rightful owner of the original digital content, or an unauthorized reselling agent.

Step 2: The vendee (V1) who wants to purchase a copy of the digital content from V may be person or an agency.

Step 3: Authentication Center (AC), who is a trusted third party supervises the whole procedure of the purchase, applies to all the applications, generates a carbon copy, and assigns digital certifications.

Step 4: The proposed carbon copy algorithm should be fair to both V and V1. That is, the proposed protocol should guarantee that V mustn't have any chance to frame V1.

Step 5: The proposed carbon copy algorithm should solve both the "customer's right problem" and the "unbinding problem".

Step 6: The proposed carbon copy algorithm should allow vendees to keep their identities anonymous during the execution of the algorithm.

Step 7: The proposed carbon copy algorithm should guarantee that both V and V1 are undeniable to their activities under this algorithm.

Step 8: The proposed carbon copy algorithm should resist to a second hand carbon copy attacks, in which a malicious vendee generates a second hand carbon copy of the content purchased and claims the ownership of it.

The architecture for the proposed technique is illustrated as follows:

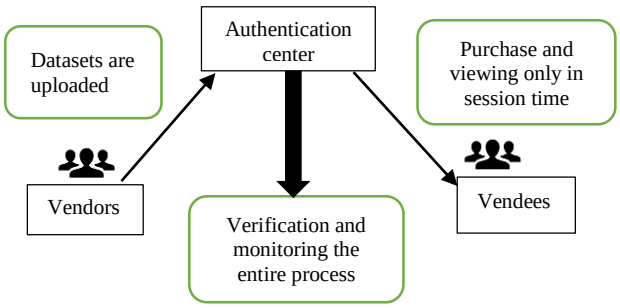

Figure 1: CCA demonstration

IV. RESULTS AND DISCUSSION

The scheduled CCA algorithm is proficient. In the suggested schema, the vendor sends the digital content just once in the enrollment part. The digital content must be encrypted before transmission between the authentication center and the vendor. Henceforth any intervention by mischievous users can be diminished. Pre distributed keys are passed down safely before encryption and decryption are done. Likewise the overhead can be reduced particularly within the situation of trading the dataset content for over just once. Digital certifications are

offered to the vendor after ratification of the datasets by the authentication center.

When we have different datasets, we apply our formula to calculate the plagiarized value by comparison with the available datasets within the database. The Plagiarized Value formula is

$$Plagiarized\ Value = \left\{1 - \frac{Diff}{Max(CS,ST)}\right\} * 100$$

Where, CS is the source dataset and TS is the target dataset

f = 14 $Max\ CS, ST$ = 19 (Length of CS)

Let's put these values in our formula

$$PlagiarizedValue = \left\{1 - \frac{Diff}{Max\,(CS,ST)}\right\} * 100 = \left\{1 - \frac{14}{19}\right\} * 100 = 26$$

$$Plagiarized\ Value = 26\ T$$

This means that 26 % is the similarity between the two datasets.

The following Figure 1 shows the comparison of protocols based on various file sizes in terms of accuracy.

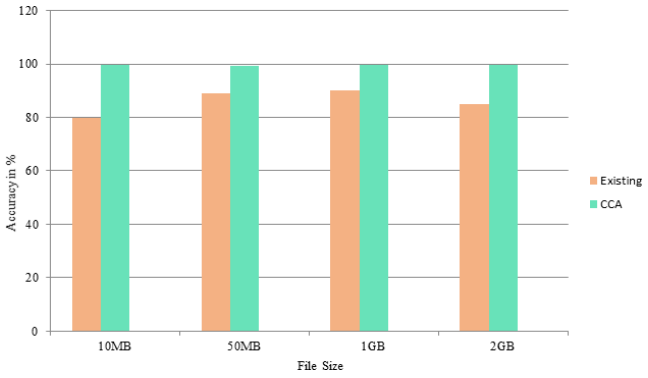

Figure 2: Comparison between existing and proposed CCA

V. CONCLUSION

This paper proffers a feasible vendee-vendor data trading protocol that enacts sufficient security, guarantees proprietorship protection and averts unlawful propagation of digital datasets. The proposed framework is highly efficient and invulnerable. The security depends on the potency of the encryption standard as well as the systematic implementation of the session timeout paradigm and several other modules involved in the suggested schema. This protocol is authentic and can be used by individuals to share digital merchandise safely without the concerns of piratism and traitor infringement. The aforesaid technique can also be used for vendee-vendor identification as well as eradicating the risks of illegal reselling of digital content. The results of the strategy revealed that data trading can be accomplished in a proficient way and can be used in numerous trading applications.

REFERENCES

[1] S. Brin, J. Davis, and H. Garcia-Molina. Copy detection mechanisms for digital documents. In SIGMOD, volume 24, pages 398–409. ACM, 1995.

[2] M. Felici, T. Koulouris, and S. Pearson. Accountability for data governance in cloud ecosystems. In CloudCom, volume 2, pages 327– 332. IEEE, 2013.

[3] T. Truderung, A. Vogt, et al. Accountability: definition and relationship to verifiability. In CCS, pages 526–535. ACM, 2010.

[4] L. Zhang, T. Jung, C. Liu, X. Ding, X.-Y. Li, and Y. Liu. Pop: Privacy preserving outsourced photo sharing and searching for mobile devices. In IEEE ICDCS. IEEE, 2015.

[5] A. Z. Broder. On the resemblance and containment of documents. In Compression and Complexity of Sequences, pages 21–29. IEEE, 1997.

[6] X. Cao, Y. Chen, and K. R. Liu. An iterative auction mechanism for data trading. In ICASSP, pages 5850–5854. IEEE, 2017.

[7] Y. Xiao. Flow-net methodology for accountability in wireless networks. Network, IEEE, 23(5):30–37, 2009.

[8] L. Zhang, X.-Y. Li, K. Liu, T. Jung, and Y. Liu. Message in a sealed bottle: Privacy preserving friending in mobile social networks. TMC, 14(9):1888–1902, 2015.

[9] S. Delgado-Segura, C. P´erez-Sol`a, G. Navarro-Arribas, and J. Herrera- Joancomart´ı. A fair protocol for data trading based on bitcoin transactions. Future Generation Computer Systems, 2017.

[10] X.-Y. Li, C. Zhang, T. Jung, J. Qian, and L. Chen. Graph-based privacy preserving data publication. In INFOCOM, pages 1–9. IEEE, 2016.