A Study on the Implementation of Encryption and Decryption Techniques towards Data mining for providing Security

Monelli Ayyavaraiah[1], Purimetla Mounitha[2]

[1]Assistant Professor, Department of Information Technology, MGIT,HYDERABAD
[2]Assistant Professor, Department of CSE, MGIT, HYDERABAD

ABSTARCT

Privacy is a standout amongst the most critical properties of an information system must fulfill, in which systems the need to share information among various, not put stock in substances, the security of sensible information has a pertinent part. In this way privacy is turning into an undeniably critical issue in numerous data mining applications. For that privacy secure distributed calculation, which was done as a major aspect of a bigger collection of research in the hypothesis of cryptography, has accomplished surprising outcomes. These outcomes were demonstrated utilizing non specific developments that can be connected to any capacity that has a proficient portrayal as a circuit. A moderately new pattern demonstrates that established access control procedures are not adequate to ensure privacy when data mining systems are utilized as a part of a malignant way. Privacy preserving data mining calculations have been as of late presented with the point of keeping the revelation of sensible information. In this paper we will depict the usage of cryptography in that data mining for privacy preserving.

Index Terms : Security, Cryptography, Privacy preserving, Distributed Data Mining

1. INTRODUCTION

Privacy preserving data mining is an imperative property that any mining system must fulfill. Up until now, on the off chance that we expected that the information in every database found in mining can be unreservedly shared. Think about a situation in which at least two gatherings owning private databases wish to run a data mining calculation on the association of their databases without uncovering any superfluous information. For instance, consider isolate therapeutic foundations that desire to lead a joint research while preserving the privacy of their patients. In this situation it is required to secure advantaged information, yet it is likewise required to empower its utilization for inquire about or for different purposes. Specifically, in spite of the fact that the gatherings understand that consolidating their data has some shared advantage, none of them will uncover its database to some other gathering.

The basic meaning of privacy in the cryptographic group constrains the information that is spilled by the distributed calculation to be the information that can be gained from the assigned yield of the calculation. In spite of the fact that there are a few variations of the meaning of privacy, with the end goal of this talk we utilize the definition that looks at the aftereffect of the genuine calculation to that of a "perfect" calculation: Consider initial a gathering that is engaged with the real calculation of a capacity (e.g. a data mining calculation). Consider additionally a "perfect situation", where notwithstanding the first gatherings there is likewise a "put stock in party" who does not veer off from the conduct that we recommend for him, and does not endeavor to swindle. In the perfect situation all gatherings send their contributions to the confided in party, who at that point processes the capacity and sends the proper outcomes to alternate gatherings. Freely, a convention is secure in the event that anything that a foe can learn in the genuine world it can

likewise learn in the perfect world, in particular from its own info and from the yield it gets from the put stock in party. Basically, this implies the convention that is keep running with a specific end goal to figure the capacity does not release any "superfluous" information.

2. PRIVACYPRESERVING

Dangerous advance in networking, storage and processor technologies has prompted the making of ultra huge database that record extraordinary measure of transactional information. Privacy issues are additionally exacerbated now that the World Wide Web makes it simple for the new data to be naturally gathered and added to databases. Privacy preserving protocols are planned so as to safeguard privacy even within the sight of antagonistic members that endeavor to accumulate information about the contributions of their associates. There are, in any case, unique levels of antagonistic conduct. Cryptographic research commonly thinks about two kinds of foes: A semi-legitimate foe (otherwise called a detached, or fair however inquisitive foe) is a gathering that effectively takes after the protocol determination, yet endeavors to take in extra information by investigating the messages got amid the protocol execution. Then again, a pernicious foe may self-assertively go astray from the protocol particular. (For instance, consider a stage in the protocol where one of the gatherings is required to pick a random number and communicate it. On the off chance that the gathering is semi-genuine then we can expect that this number is for sure random. Then again, if the gathering is pernicious, at that point he may pick the number adroitly that empowers him to increase extra information.) It is obviously less demanding to plan an answer that is secure against semi-legit enemies, than it is to outline an answer for noxious foes.

A typical approach is in this way to first outline a safe protocol for the semi-legit case, and then change it into a protocol that is secure against pernicious foes. This change should be possible by requiring each gathering to utilize zero-information verifications to demonstrate that each progression that it is taking takes after the detail of the protocol. More productive changes are regularly required, since this nonexclusive approach may be somewhat wasteful and add significant overhead to each progression of the protocol. We comment that the semi-fair antagonistic model is regularly a sensible one. This is on account of digressing from a predefined program which might be covered in a mind boggling application is a non-minor undertaking, and on the grounds that a semi-genuine ill-disposed conduct can show a situation in which the gatherings that take an interest in the protocol are straightforward, yet following the protocol execution an enemy may acquire a transcript of the protocol execution by breaking into a machine utilized by one of the members.

3. PRIVACY PRESERVINGCOMPUTATION

In this segment we will portray the different calculation methods which we are utilizing for data.

3.1 Classification

Alice has a private database D1 and Bob has private database D2. In what capacity would alice be able to and Bob manufacture a choice tree in light of D1 D2 without revealing the substance of their private database to each other? A few calculations like ID3, Gain Ratio, Gini Index and numerous other can be utilized for Decision Tree.

3.2 Data Clustering

Alice has a private database D1 and Bob has private database D2. Alice and Bob need to mutually perform data clustering on D1 D2. This is fundamentally in view of data clustering rule that tries to increment intra class similitude and limit interclass closeness.

3.3 Mining Association Rules

Let Alice has a private database D1 and Bob has private database D2. On the off chance that Alice and Bob wish to together discover the association rules from D1 D2 without uncovering the information from singular databases.

3.4 Data Generalization, Summarization and Characterization

Let Alice has a private database D1 and Bob has private database D2. On the off chance that they wish to together perform data generalization, summarization or characterization on their joined database D1 D2, at that point this issue turns into a Secure Multiparty Communication issue.

3.5 Profile Matching

Alice has a database of programmer's profile. Weave has as of late followed a conduct of a man, whom he speculates a programmer. Presently, if Bob needs to check whether his uncertainty is right, he needs to check Alice's database. Alice's database should be ensured in light of the fact that it contains programmer's connected touchy information. In this manner, when Bob enters the programmer's conduct and quests the Alice's database, he can't see his entire database, yet rather, just gets the examination consequences of the matching conduct.

3.6 Fraud Detection

Two noteworthy budgetary associations need to participate in anticipating fraudulent interruptions into their registering system, without sharing their data designs, since their individual private database contains touchy data.

4. SECURE COMPUTATION AND PRIVACY PRESERVING DATAMINING

There are two particular issues that emerge in the setting of privacy-preserving data mining. The first is to choose which capacities can be securely processed, where wellbeing implies that the privacy of people is safeguarded. For instance, is it safe to register a choice tree on classified data in an association and announce the subsequent tree? Generally, we will accept that the consequence of the data mining calculation is either protected or considered fundamental. Hence, the inquiry turns out to be the means by which to process the outcomes while limiting the harm to privacy. For instance, it is constantly conceivable to pool the greater part of the data in a single place and run the data mining calculation on the pooled data. Be that as it may, this is precisely what we would prefer not to. Consequently, the inquiry we deliver is the way to register the outcomes without pooling the data, and in a way that uncovers only the last consequences of the data mining calculation. This inquiry of privacy-preserving data mining is really an extraordinary instance of a since quite a while ago contemplated issue in cryptography called secure multiparty calculation. This issue manages a setting where an arrangement of gatherings with private information sources wish to together register some capacity of their data sources. Freely, this joint calculation ought to host the property that the gatherings take in the right yield and that's it, regardless of whether a portion of the gatherings noxiously connive to acquire more information. Obviously, a protocol that gives this certification can be utilized to take care of privacy-preserving data mining issues of the sort talked about above.

5. CRYPTOGRAPHY: OBLIVIOUSTRANSFER

We depict here consequences of a collection of cryptographic research that shows how isolate gatherings can mutually process any capacity of their contributions, without uncovering some other information. As we contended over, these outcomes accomplish maximal privacy that conceals all information aside from the assigned yield of the capacity. This collection of research endeavors to display the world in a way which is both reasonable and general. While there are a few parts of "this present reality" that are not demonstrated by this examination, the privacy ensures and the sweeping statement of the outcomes are very momentous.

Absent exchange is a fundamental protocol that is the principle building piece of secure calculation. It may appear to be abnormal at initially, yet its part in secure calculation ought to wind up clear later. (Truth be told, it was appeared by Kilian [11] that unaware exchange is adequate for secure calculation as in given a usage of unmindful exchange, and no other

cryptographic crude, one could develop any safe calculation protocol.)

Unaware exchange is frequently the most computationally escalated activity of secure protocols, and is rehashed commonly. Every conjuring of negligent exchange commonly requires a consistent number of summons of trapdoor stages (i.e. open key activities, or exponentiations). It is conceivable to decrease the amortized overhead of unaware exchange to one exponentiations for every a logarithmic number of unmindful exchanges, notwithstanding for the instance of vindictive enemies [15].

The issue of "neglectful polynomial assessment" (OPE) includes a sender and a collector. The sender's information is a polynomial Q of degree k over some limited field *f* and the

recipient's info is a component z c *f* (the degree k of Q is open). The protocol is to such an extent that the recipient gets Q (z) without getting the hang of whatever else about the polynomial Q, and the sender adapts nothing. That is, the issue considered is the private calculation of the capacity (Q, z) → (,Q (z)). This issue was presented in [14], where a proficient arrangement was additionally exhibited. The overhead of that protocol is O (k) exponentiations (utilizing strategies proposed in [15]). (Note that this protocol keeps up privacy even with a noxious foe. In the semi-fair case a less complex OPE protocol can be composed in light of any homomorphic encryption conspire, with an overhead of O (k) calculation and O(k | *f* |) correspondence.)

The primary inspiration for utilizing OPE is to use the way that the yield of a k degree polynomial is (k + 1)- savvy free. Another inspiration is that polynomials can be utilized for approximating capacities that are characterized over the Real numbers.

6. THE TWO-PARTY CASE

Yao's two-party protocol is truly productive, as long as the span of the sources of info, and the extent of the circuit registering the capacity, are sensible. Indeed, for some capacities the effectiveness of Yao's non specific protocol is tantamount to that of protocols that are focused for processing the particular capacity. We portray here a distributed situation of registering the ID3 calculation, where Yao's protocol is clearly too expensive. Then again, a particular protocol can be intended for registering this calculation, which utilizes Yao's protocol as a crude.

We are occupied with a situation including two gatherings, every last one of them holding a database of various exchanges, where every one of the exchanges have a similar arrangement of properties (this situation is additionally indicated as an "on a level plane divided" database). The gatherings wish to figure a choice tree by applying the ID3 calculation to the association of their databases.

An innocent approach for executing a privacy preserving arrangement is to apply the non specific Yao protocol to the ID3 calculation. This approach experiences two noteworthy obstructions. To begin with, the extent of the databases is ordinarily expansive. As every exchange can have numerous properties, and there may be a huge number of exchanges, the encoding of each gathering's information may require a huge number of bits. This implies the computational overhead of running a negligent exchange for every info bit may be high.

Most cryptographic protocols, be that as it may, register works over limited fields. Regardless of whether the circuit figures a guess to the logarithm, this calculation includes assessing polynomials and consequently requires processing duplications and exponentiations. An extra issue is that running ID3 includes numerous rounds. The piece of the circuit processing the ith round relies upon the consequences of the past i−1 rounds. A gullible execution could require an encoding of numerous duplicates of this progression, every last one of them comparing to a particular consequence of the past rounds.

A key perception is that every hub of the tree can be registered independently, with the yield made open, before proceeding to the following hub. When all is said in done, private protocols have the property that halfway esteems stay covered up. Nonetheless, on account of ID3 some of these middle of the road esteems (particularly, the assignments of credits to hubs) are entirely of the yield and may in this way be uncovered. Once the quality of a given hub has been discovered, the two gatherings can independently segment their residual exchanges appropriately for the coming recursive calls. This implies private distributed ID3 can be decreased to secretly finding the trait with the most elevated information pick up. (This is a somewhat streamlined contention as alternate strides of ID3 should likewise be precisely managed. In any case, the principle issues emerge inside this progression.)

The overhead of the protocol depicted above includes:

- Alice and Bob participating in an unaware exchange protocol for each information wire of the circuit that is related with Bob's information,
- Alice sending Bob tables of size straight in the span of the circuit,
- Bob unscrambling a steady number of figure writings for each door of the circuit (this is the cost brought about in assessing the entryways).

The calculation overhead is ruled by the unaware exchange organize, since the assessment of the entryways utilizes symmetric encryption which is exceptionally effective contrasted with careless exchanges that require measured exponentiations (this holds for little circuits; if the circuit is huge then the circuit calculation may start to command). The calculation overhead is consequently generally straight in the length of Bob's information. The quantity of rounds of the protocol is steady. (to be specific, the variation depicted here has two rounds utilizing the two-round absent exchange protocols of [5, 6, 15]).

The correspondence overhead is direct in the measure of the circuit. (The variation of the protocol depicted in [22], which gives security against pernicious foes, requires sending s duplicates of the circuit to constrain the likelihood of swindling to be exponentially little in s. See likewise [17] for an alternate variation, which gives security against malevolent foes at the cost of applying open key tasks for each entryway.)

A central point commanding the overhead is, subsequently, the span of the circuit portrayal of f. There are numerous capacities for which we don't know how to make direct size circuits (e.g. capacities processing increases or exponentiations, or capacities that utilization aberrant tending to). In any case, there are numerous different capacities, quite those including increments and correlations, which can be registered by direct size circuits. The span of the info ought to likewise be sensible. For instance, we can't expect that two gatherings, every one of them holding a database with a great many passages, could run the protocol for processing a capacity whose sources of info are the whole databases.

7. THE MULTI-PARTYCASE

The multi-party case includes at least three gatherings that desire to register some capacity of their contributions without releasing any pointless information. In the multi-party situation, there are protocols that empower the gatherings to register any joint capacity of their contributions without uncovering some other information about the data sources. That is, process the capacity while accomplishing an indistinguishable privacy from in the perfect model. This was appeared to be conceivable on a basic level by Goldreich, Micali and Wigderson [10], Ben-Or, Goldwasser and Wigderson [3], and by Chaum, Crepau and Damgard [4], for various situations. These developments, as well, depend on speaking to the processed capacity as a circuit and assessing it. The developments do have, notwithstanding, some extra disadvantages, contrasted with the two-

party case:

- The calculation and correspondence overhead of the protocol is direct in the span of the circuit, and the quantity of correspondence rounds relies upon the profundity of the circuit1, dissimilar to the two-party situation where the quantity of rounds is consistent. Moreover, the protocol that is keep running for each door of the circuit is more perplexing than the calculation of an entryway in the two-party case, particularly in the vindictive party situation, and requires open key tasks (in spite of the fact that the overhead is as yet polynomial).

- The multi-party protocols require each match of gatherings to trade messages (keeping in mind the end goal to process each door of the circuit). The required correspondence chart is, subsequently, an entire diagram, while a meager correspondence diagram could have been adequate if no security was required. In numerous applications, for instance applications keep running between a web server and numerous customers, it is difficult to require all sets of gatherings to impart.

- The security of the multi-party protocols is guaranteed insofar as there is no degenerate coalition of in excess of one half or 33% of the gatherings (contingent upon the situation). Much of the time, nonetheless, it is difficult to guarantee that the quantity of degenerate parties is littler than such a limit (for instance, consider a web application in which anybody can enlist and take an interest, and which, in this manner, empowers a foe to enlist any number of degenerate members). In such cases the security of the protocol isn't ensured.

Contrasted with the two-party case, be that as it may, it is harder to apply the bland developments to real situations. To outline this point we think about the instance of running a protected calculation for processing the consequence of a bartering, where there is a conspicuous inspiration for privacy and security, and likewise certain confinements on the task of the gatherings. The closeout application, talked about in [16], isn't identified with data mining, yet it exemplifies a portion of the troubles of the multiparty case. The exchange underneath applies for any capacity that can be figured by a circuit of sensible size.

The bartering situation is that of a "fixed offer" closeout, and comprises of a barker and numerous bidders. Every bidder presents a solitary mystery offer (i.e. the offer is fixed in an envelope). There is a known choice manage, whose information sources are the submitted offers, and whose yield is the character of the triumphant bidder and the sum that this bidder needs to pay. For instance, in an "English closeout" the triumphant bidder is the bidder who offered the most noteworthy offer, and he needs to pay the measure of his offer. In the second-cost, or Vickrey, kind of closeout (which has some pleasant properties that are outside the extent of this paper) the champ is the most elevated bidder and he needs to pay the measure of the second most astounding offer. Offering is permitted until some point in time, and at that stage the choice lead is connected to the submitted offers.

In the physical world offers are submitted in fixed envelopes that are kept secure until the finish of the offering time frame, and are then opened by the barker. In the virtual world we might want to keep the offers mystery amid the offering time frame, yet we could likewise endeavor to shroud all information subsequently, aside from the character of the triumphant party and the sum he needs to pay. For instance, on account of a Vickrey closeout the barker's yield could be restricted to the personality of the most astounding bidder (yet not the estimation of his offer), and the estimation of the second most astounding offer (yet not the character of the second most noteworthy bidder). This is more privacy than can be accomplished in the physical world. (Truth be told, a portion of the proposed clarifications at the disagreeability of second cost barters depend on conceivable assaults that a pernicious barker can mount on the off chance that he takes in the offer estimation of the most noteworthy bidder. This marvel is unavoidable in reality, yet can be kept away from if a privacy preserving protocol is utilized to process the consequence of the sale.)

Privacy preserving multi-party calculation can be lessened to the two-party case. To be specific, it is conceivable to utilize the non specific two-party protocol to register a capacity in the multi-party situation. Such a diminishment is depicted in [16]. Before portraying the features of the lessening we initially depict the upsides of this approach.

7.1 Trust

Keeping in mind the end goal to utilize the two-party development it is expected that there are two extraordinary gatherings, and privacy is protected as long as these two gatherings don't intrigue. Specifically, a conspiracy of any number of gatherings (even a dominant part of the gatherings) that does exclude both extraordinary gatherings does not influence the privacy and security of the protocol. Protocols with this security affirmation may appear to be weaker than protocols that are secure against arrangements of say, any coalition of short of what one portion of the gatherings. All things considered, there is a coalition of only two gatherings – the two extraordinary gatherings, can break the security of the system. Consider however a situation where a large portion of the gatherings are clients (e.g. bidders) that have not built up trust connections amongst themselves, and there are at least one focal gatherings that are more settled. For instance, in the bartering situation we can accept that the two unique gatherings are the salesperson and another gathering which we mean as the "guarantor", and which can be, for instance, a bookkeeping firm. We realize that a foe can enlist numerous phony bidders with a specific end goal to control a larger part of the taking an interest parties. It appears to be harder, however, for the enemy to have the capacity to control insiders of both extraordinary gatherings, i.e. in the barker's association and in the bookkeeping firm.

7.2 Independence of Inputs

Debased gatherings must pick their inputs autonomously of the genuine gatherings' inputs. This property is critical in a fixed closeout, where offers are kept mystery and gatherings must fix their offers autonomously of others. We take note of that independence of inputs isn't suggested by privacy. For instance, it might be conceivable to produce a higher offer, without knowing the estimation of the first one. Such an assault can really be completed on some encryption plans.

7.3 Communication

We can outline the lessening to such an extent that each of the "straightforward" taking an interest gatherings should just speak with one of the exceptional gatherings (e.g. the barker), and should just send a solitary message to this gathering. This property incredibly improves the required communication framework, and empowers to run the protocol without requiring all gatherings to be online in the meantime (truth be told, contrasted with a protocol that gives no security by any stretch of the imagination, the main new communication channel that is presented by the safe protocol is the channel between the two unique gatherings). At the point when all the "straightforward" gatherings wrap up their messages, the two uncommon gatherings run a short protocol to finish the calculation of the capacity.

7.4 Privacy

No gathering ought to get the hang of much else besides its recommended output. Specifically, the main information that ought to be found out about other gatherings' inputs is the thing that can be gotten from the output itself. For instance, in a bartering where the main offer uncovered is that of the most noteworthy bidder, it is unmistakably conceivable to infer that every single other offer were lower than the triumphant offer. Be that as it may, this ought to be the main information uncovered about the losing offers.

7.5 Correctness

Each gathering is guaranteed that the output that it gets is right. To proceed with the case of a closeout, this infers the gathering with the most noteworthy offer is guaranteed to win, and no gathering including the barker can adjust this.

7.6 Efficiency

The protocol assesses a circuit portrayal of the capacity. The overhead per entryway and per input bit is as in the two-party development, and is lower than in the multi-party developments.

7.7 Guaranteed Output Delivery

Tainted gatherings ought not have the capacity to keep fair gatherings from getting their output. As such, the enemy ought not have the capacity to disturb the calculation via completing a "refusal of administration" assault.

7.8 Fairness

Defiled gatherings ought to get their outputs if and just if the legit parties additionally get their outputs. The situation where an undermined party acquires output and a genuine gathering does not ought not be permitted to happen. This property can be significant, for instance, on account of agreement marking. In particular, it would be exceptionally tricky if the debased party got the marked contract and the fair party did not.

The protocol is keep running with the two extraordinary gatherings playing the parts of the two gatherings in the two-party case. The guarantor readies a circuit for registering the capacity. This circuit may host numerous inputs of various gatherings – for instance, the inputs may be the offers of the diverse bidders. The guarantor encodes the circuit as in the two-party case, by picking distorted esteems for the wires and getting ready tables for each entryway. The other unique gathering (the barker) is

in charge of processing the consequence of the circuit. So as to do that it ought to get the tables that were set up by the backer, and one jumbled an incentive for each information wire, in particular the esteem that relates to the information bit related with that wire. When it gets the distorted estimations of all information wires it can register the output of the circuit.

Given the intermediary unmindful exchange protocol, whatever is left of the usage is straightforward. Every bidder takes part in an intermediary neglectful exchange for every one of its information bits. The contribution of the bidder to this protocol is the estimation of the info bit. The sender is the backer, and its two inputs are the two jumbled esteems that are related with the comparing input wire. The beneficiary is the salesperson, and it takes in the jumbled esteem that relates to the info bit. This protocol comprises of a solitary message that is sent from the bidder to the salesperson, and then a series of communication between the barker and the guarantor. The barker can really hold up until the point that it gets messages from every one of the bidders previously it runs the round of communication with the guarantor in parallel for all information bits. The fundamental computational overhead of the protocol is brought about by the intermediary unmindful exchanges, and is the same as in the two-party case – an intermediary negligent exchange must be executed for each information wire. Gauges in [16] demonstrate that this technique can be utilized to safely actualize Vickrey barters that include many bidders.

8. CONCLUSIONS

Cryptographic protocols for secure calculation accomplished noteworthy outcomes: it was demonstrated that non specific developments can be utilized to figure any capacity safely and it

was likewise exhibited that a few capacities can be processed much more proficiently utilizing particular developments. In any case, a protected protocol for processing a specific capacity will dependably be more expensive than a credulous protocol that does not give any security. By making utilization of cryptographic methods to store delicate data and giving access to the put away data in view of a person's part, we guarantee that the data is protected from privacy ruptures. This paper was expected to exhibit essential thoughts from an extensive group of cryptographic research on secure distributed calculation, and their applications to data mining. We depicted in a nutshell the meanings of security, and the bland developments for the two-party and multi-party situations. We demonstrated that it is simpler to plan an execution in view of the developments for the two-party case than it is to outline one in light of the multi-party developments. The fundamental parameter that influences the practicality of actualizing a protected protocol in light of the bland developments is the measure of the best combinatorial circuit that processes the capacity that is assessed. We trust that further research here is essential for the improvement of secure and proficient protocols in this field.

REFERENCES

[1]D. Beaver, S. Micali and P. Rogaway, The round intricacy of secure protocols, Proc. of 22nd ACM Symposium on Theory of Computing (STOC), pp. 503-513, 1990.

[2]M. Bellare and S. Micali, Non-Interactive Oblivious Transfer and Applications, Advances in Cryptology - CRYPTO '89. Address Notes in Computer Science, Vol. 435, Springer-Verlag, 1997, pp. 547-557.

[3]M. Ben-Or, S. Goldwasser and A. Wigderson, Completeness hypotheses for non cryptographic blame tolerant distributed calculation, Proceedings of the twentieth Annual Symposium on the Theory of Computing (STOC), ACM, 1988, pp. 1– 9.

[4]D. Chaum, C. Crepeau and I. Damgard, Multiparty genuinely secure protocols, Proceedings of the twentieth Annual Symposium on the Theory of Computing (STOC), ACM, 1988, pp. 11– 19.

[5]S. Indeed, O. Goldreich and A. Lempel. A Randomized Protocol for Signing Contracts. Communications of the ACM, 28(6):637-647, 1985.

[6]O. Goldreich. Establishments of Cryptography: Volume 2 { Basic Applications. Cambridge University Press, 2004

[7]Jaideep Vaidya and Chris Clifton, "Utilizing the 'multi' in Secure Multiparty Computation," WPES'03 October 30, 2003, Washington, DC, USA, ACM Transaction 2003, pp120-128.

[8]Chris Clifton, Murat Kantarcioglu, Jaideep Vaidya, Xiaodong Lin, Michael Y. Zhu, "Apparatuses for Privacy Preserving Data Mining". universal meeting on learning revelation and data mining, Vol. 4, No. 2, 2002, pp. 1-8.

[9]Anand Sharma and vibha ojha ""Privacy preserving Data Mining by Cryptography" in Springer-LNCS-CICS-Vol:89, "Late Trends in Network Security and Applications" .pp.576-581.2010.

[10]O. Goldreich, S. Micali and A. Wigderson, How to Play any Mental Game - A Completeness Theorem for Protocols with Honest Majority, Proceedings of the nineteenth Annual Symposium on the Theory of Computing (STOC), ACM, 1987, pp. 218– 229.

[11]J. Kilian, Founding cryptography on careless exchange, ACM STOC '88, pp. 20-31.

[12]Y. Lindell and B. Pinkas, Privacy Preserving Data Mining, Journal of Cryptology, Vol. 15, No. 3, pp. 177-206, 2002.

[13]M. Luby, Pseudorandomness and Cryptographic Applications, Princeton Computer Science Notes, 1996.

[14]M. Naor and B. Pinkas, Oblivious Transfer and Polynomial Evaluation, Proceedings of the 31th Annual Symposium on the Theory of Computing (STOC), ACM, 1999, pp. 245– 254.

[15]M. Naor and B. Pinkas, Efficient Oblivious Transfer Protocols, Proceedings of twelfth SIAM Symposium on Discrete Algorithms (SODA), January 7-9 2001, Washington DC, pp. 448– 457.

[16]M. Naor, B. Pinkas and R. Sumner, Privacy Preserving Auctions and Mechanism Design, Proc. of the first ACM meeting on Electronic Commerce, November 1999.

[17]S. Jarecki and V. Shmatikov. Eficient Two-Party Secure Computation on Committed Inputs. In EUROCRYPT 2007, Springer-Verlag (LNCS 4515), pages 97-114, 2007.

[18]Rebecca Wright, "Advance on the PORTIA Project in Privacy Preserving Data Mining," A data reconnaissance and privacy insurance workshop hung on third June 2008.

[19]M. O. Rabin, How to trade privileged insights by unaware exchange, Technical Memo TR-81, Aiken Computation Laboratory, 1981.

[20]J.E. Savage, Computational work and time on limited machines, Journal of the ACM, 19(4), pp. 660-674, 1972.

[21]A. C. Yao, How to produce and trade mysteries, Proceedings 27th Symposium on Foundations of Computer Science (FOCS), IEEE,

1986, pp. 162– 167.

[22] Y. Lindell and B. Pinkas. An Eficient Protocol for Secure Two-Party Computation in the Presence of Malicious Adversaries In EUROCRYPT 2007, Springer-Verlag (LNCS 4515), pages 52-78, 2007.
[23] B. Srinivas, Shoban Babu Sriramoju, "A Secured Image Transmission Technique Using Transformation Reversal" in "International Journal of Scientific Research in Science and Technology", Volume-4, Issue-2, February-2018, 1388-1396 [Print ISSN: 2395-6011 | Online ISSN: 2395-602X]

[24] B. Srinivas Gadde Ramesh, Shoban Babu Sriramoju, "A Study on Mining Top Utility Itemsets In A Single Phase" in "International Journal for Science and Advance Research in Technology (IJSART)", Volume-4, Issue-2, February-2018, 1692-1697, [ISSN(ONLINE): 2395-1052]

[25] Monelli Ayyavaraiah, "Review of Machine Learning based Sentiment Analysis on Social Web Data" in "International Journal of Innovative Research in Computer and Communication Engineering" Vol 4,Issue 6,March 2016 [ISSN(online) : 2320-9801, ISSN(print) : 2320-9798]
[26] B. Srinivas, Gadde Ramesh, Shoban Babu Sriramoju, "An Overview of Classification Rule and Association Rule Mining" in "International Journal of Scientific Research in Computer Science, Engineering and Information Technology", Volume-3, Issue-1, February-2018, 643-650, [ISSN : 2456-3307]
[27] B. Srinivas, Shoban Babu Sriramoju, "Managing Big Data Wiki Pages by Efficient Algorithms Implementing In Python" in "International Journal for Research in Applied Science & Engineering Technology (IJRASET)", Volume-6, Issue-II, February-2018, 2493-2500, [ISSN : 2321-9653]
[28] Shoban Babu Sriramoju, "Analysis and Comparison of Anonymous Techniques for Privacy Preserving in Big Data" in "International Journal of Advanced Research in Computer and Communication Engineering",Vol 6, Issue 12, December 2017, DOI 10.17148/IJARCCE.2017.61212 [ISSN(online) : 2278-1021, ISSN(print) : 2319-5940]
[29] Monelli Ayyavaraiah, " A Study on Large-Scale Cross-Media Retrieval of Wikipedia Images towards Visual Query and Textual Expansion" in "International Journal for Research in Applied Science and Engineering Technology", Volume-6, Issue-II, February 2018, 1238-1243 [ISSN : 2321-9653], www.ijraset.com
[30] Shoban Babu Sriramoju, " Review on Big Data and Mining Algorithm" in "International Journal for Research in Applied Science and Engineering Technology", Volume-5, Issue-XI, November 2017, 1238-1243 [ISSN : 2321-9653], www.ijraset.com

[31] Shoban Babu Sriramoju, "OPPORTUNITIES AND SECURITY IMPLICATIONS OF BIG DATA MINING" in "International Journal of Research in Science and Engineering",Vol 3, Issue 6, Nov-Dec 2017 [ISSN : 2394-8299].
[32] Shoban Babu Sriramoju, "Heat Diffusion Based Search for Experts on World Wide Web" in "International Journal of Science and Research", https://www.ijsr.net/archive/v6i11/v6i11.php, Volume 6, Issue 11, November 2017, 632 - 635, #ijsrnet
[33] Monelli Ayyavaraiah, "Nomenclature of Opinion Miningand Related Benchmarking Tools" in "International Journal of Scientific & Engineering Research" Vol 7,Issue 8, February 2018, [ISSN 2229-5518]
[34] Dr. Shoban Babu Sriramoju, Prof. Mangesh Ingle, Prof. Ashish Mahalle "Trust and Iterative Filtering Approaches for Secure Data Collection in Wireless Sensor Networks" in "International Journal of Research in Science and Engineering" Vol 3, Issue 4, July-August 2017 [ISSN : 2394-8299].
[35] Siripuri Kiran, 'Decision Tree Analysis Tool with the Design Approach of Probability Density Function towards Uncertain Data Classification', International Journal of Scientific Research in Science and Technology(IJSRST), Print ISSN : 2395-6011, Online ISSN : 2395-602X,Volume 4 Issue 2, pp.829-831, January-February 2018. URL : http://ijsrst.com/IJSRST1841198
[36] Namavaram Vijay, Ajay Babu Sriramoju, Ramesh Gadde, "Two Layered Privacy Architecture for Big Data Framework" in "International Journal of Innovative Research in Computer and Communication Engineering"
Vol 5, Issue 10, October 2017 [ISSN(online) : 2320-9801, ISSN(print) : 2320-9798]
[37] Dr. Shoban Babu, Prof. Mangesh Ingle, Prof. Ashish Mahalle, "HLA Based solution for Packet Loss Detection in Mobile Ad Hoc Networks" in "International Journal of Research in Science and Engineering" Vol 3, Issue 4,July-August 2017 [ISSN : 2394-8299].
[38] Shoban Babu Sriramoju, "A Framework for Keyword Based Query and Response System for Web Based Expert Search" in "International Journal of Science and Research" Index Copernicus Value(2015):78.96
[ISSN : 2319-7064].
[39] Ajmera Rajesh, Siripuri Kiran, "Anomaly Detection Using Data Mining Techniques in Social Networking" in "International Journal for Research in Applied Science and Engineering Technology", Volume-6, Issue-II, February 2018, 1268-1272 [ISSN : 2321-9653], www.ijraset.com

[40] Sriramoju Ajay Babu, Dr. S. Shoban Babu, "Improving Quality of Content Based Image Retrieval with Graph Based Ranking" in "International Journal of Research and Applications" Vol 1, Issue 1,Jan-Mar 2014 [ISSN : 2349-0020].
[41] Dr. Shoban Babu Sriramoju, Ramesh Gadde, "A Ranking Model Framework for Multiple Vertical Search Domains" in "International Journal of Research and Applications" Vol 1, Issue 1,Jan-Mar 2014 [ISSN : 2349-0020].
[42] Mounika Reddy, Avula Deepak, Ekkati Kalyani Dharavath, Kranthi Gande, Shoban Sriramoju, "Risk-Aware Response Answer for Mitigating Painter Routing Attacks" in "International Journal of Information Technology and Management" Vol VI, Issue I, Feb 2014 [ISSN : 2249-4510]
[43] Mounica Doosetty, Keerthi Kodakandla, Ashok R, Shoban Babu Sriramoju, "Extensive Secure Cloud Storage System Supporting Privacy-Preserving Public Auditing" in "International Journal of Information Technology and Management" Vol VI, Issue I, Feb 2012 [ISSN : 2249-4510]
[44] Shoban Babu Sriramoju, "An Application for Annotating Web Search Results" in "International Journal of Innovative Research in Computer and Communication Engineering" Vol 2,Issue 3,March 2014
[ISSN(online) : 2320-9801, ISSN(print) : 2320-9798]
[45] Siripuri Kiran, Ajmera Rajesh, "A Study on Mining Top Utility Itemsets In A Single Phase" in "International Journal for Science and Advance Research in Technology (IJSART)", Volume-4, Issue-2, February-2018, 637-642, [ISSN(ONLINE): 2395-1052]

[46] Shoban Babu Sriramoju, "Multi View Point Measure for Achieving Highest Intra-Cluster Similarity" in "International Journal of Innovative Research in Computer and Communication Engineering" Vol 2,Issue 3,March 2014 [ISSN(online) : 2320-9801, ISSN(print) : 2320-9798]
[47] Ramesh Gadde, Namavaram Vijay, "A SURVEY ON EVOLUTION OF BIG DATA WITH HADOOP" in "International Journal of Research in Science and Engineering",Vol-3, Issue-6, Nov-Dec 2017, 92-99 [ISSN : 2394-8299].
[48] Amitha Supriya. "Implementation of Image Processing System using Big Data in the Cloud Environment." International Journal for Scientific Research and Development 5.10 (2017): 211-217.
[49] SA Supriya. "A Survey Model of Big Data by Focusing on the Atmospheric Data Analysis." International Journal for Scientific Research and Development 5.10 (2017): 463-466.
[50] Shoban Babu Sriramoju, Madan Kumar Chandran, "UP-Growth Algorithms for Knowledge Discovery from Transactional Databases" in "International Journal of Advanced Research in Computer Science and Software Engineering", Vol 4, Issue 2, February 2014 [ISSN : 2277 128X]
[51] Shoban Babu Sriramoju, Azmera Chandu Naik, N.Samba Siva Rao, "Predicting The Misusability Of Data From Malicious Insiders" in "International Journal of Computer Engineering and Applications" Vol V,Issue II,Febrauary 2014 [ISSN : 2321-3469]
[52] Ajay Babu Sriramoju, Dr. S. Shoban Babu, "Analysis on Image Compression Using Bit-Plane Separation Method" in "International Journal of Information Technology and Management", Vol VII, Issue X, November 2014 [ISSN : 2249-4510]
[53] Shoban Babu Sriramoju, "Mining Big Sources Using Efficient Data Mining Algorithms" in "International Journal of Innovative Research in Computer and Communication Engineering" Vol 2, Issue 1,January 2014 [ISSN(online) : 2320-9801, ISSN(print) : 2320-9798]
[54] Ajay Babu Sriramoju, Dr. S. Shoban Babu, "Study of Multiplexing Space and Focal Surfaces and Automultiscopic Displays for Image Processing" in "International Journal of Information Technology and Management"Vol V, Issue I, August 2013 [ISSN : 2249-4510]
[55] Dr. Shoban Babu Sriramoju, "A Review on Processing Big Data" in "International Journal of Innovative Research in Computer and Communication Engineering" Vol-2, Issue-1, January 2014 [ISSN(online) : 2320-9801, ISSN(print) : 2320-9798]
[56] Namavaram Vijay, S Ajay Babu, "Heat Exposure of Big Data Analytics in a Workflow Framework" in "International Journal of Science and Research", Volume 6, Issue 11, November 2017, 1578 - 1585, #ijsrnet
[57] Shoban Babu Sriramoju, Dr. Atul Kumar, "An Analysis around the study of Distributed Data Mining Method in the Grid Environment : Technique, Algorithms and Services" in "Journal of Advances in Science and Technology" Vol-IV, Issue No-VII, November 2012 [ISSN : 2230-9659]
[58] Shoban Babu Sriramoju, Dr. Atul Kumar, "An Analysis on Effective, Precise and Privacy Preserving Data Mining Association Rules with Partitioning on Distributed Databases" in "International Journal of Information Technology and management" Vol-III, Issue-I, August 2012 [ISSN : 2249-4510]
[59] Shoban Babu Sriramoju, Dr. Atul Kumar, "A Competent Strategy Regarding Relationship of Rule Mining on Distributed Database Algorithm" in "Journal of Advances in Science and Technology" Vol-II, Issue No-II, November 2011 [ISSN : 2230-9659]
[60] Ajay Babu Sriramoju, Namavaram Vijay, Ramesh Gadde, "SKETCHING-BASED HIGH-PERFORMANCE BIG DATA PROCESSING ACCELERATOR" in "International Journal of Research in Science and Engineering",Vol-3, Issue-6, Nov-Dec 2017, 92-99 [ISSN : 2394-8299].
[61] Shoban Babu Sriramoju, Dr. Atul Kumar, "Allocated Greater Order Organization of Rule Mining utilizing Information Produced Through Textual facts" in "International Journal of Information Technology and management" Vol-I, Issue-I, August 2011 [ISSN : 2249-4510]