ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 1, Issue 3, November 2014

Investigations on Methods Evolved for Protecting Sensitive Data

K.Deepika[1], P.Andrew[2], R.Santhya[3], Prof.S.Balamurugan[4], S.Charanyaa[5]

Department of IT, Kalaignar Karunanidhi Institute of Technology, Coimbatore, TamilNadu, India[1,2,3,4]

Senior Software Engineer Mainframe Technologies Former, L&T Infotech, Chennai, TamilNadu, India[5]

Abstract: This paper reviews strategies evolved for protecting sensitive data for the past 10 years. There has been a steep rise in privacy concerns in today's Internet world. There is a definitive need to provide confidentiality as well as preserve privacy of sensitive data. Confidentiality means that data stored in one place unauthorized is difficulty of impossible to access. Usually confidentiality is achieved by be using access policy or used some cryptographic tools. Privacy means the safety provided to the information, without leaking sensitive information. Considering the case of a medical database to join with a research institution. In that case patient's personal health care information and medical information have to be provided for researchers. Hence, in order to provide every patient record privacy, the database needs to be an anonymized version of the patient record then sent to the researchers. Researchers are provided with anonymized database only. The Evolution of Sensitive Data Preservation techniques are discussed. The sensitive data attack prevention techniques are portrayed. Techniques to protect trajectory sensitive data are also intensively discussed.

Keywords: Data Confidentiality, Cryptography, Sensitive Data, k-anonymity, Attack Prevention, Trajectory Sensitive Data

I. INTRODUCTION

k-anonymization optimization algorithm, serves as a vital privacy protection mechanism in data privacy preservation. Apart from homogeneity background knowledge attacks to which k-anonymization is vulnerable to, it considers only single static release, thereby protecting data up to the first release or the first recipient only but in practice, data sources are dynamically growing rapidly everyday and everyhour, and the updated data may be published as and when updated at the same time preserving the anonymity. An improved method for privacy protection proposed in the literature is sky stream k-anonymity facilitating k-anonymity on data streams. The problem encountered in such microdata database is controversy between the database owner and the users or organizations interacting with the database the issue to be solved here is to decide whether the updated database, preserves individual privacy even without the database owner, directly knowing what the new data to be updated is. We consider Alice to be owner of a k-anonymized version of the microdata database, and it is needed to determine whether the database, after inserting a tuple owned by Bob, is still preserving the k-anonymity. This work discusses an investigation on commutative, product homomorphic encryption protocol that rely on the suppression and generalization based k-anonymous database that is built on an enhanced Diffie-Hellman key exchange algorithm which ensures privacy preserving updated to microdata databases.

The remainder of the paper is organized as follows. Section 2 deals about definition and primitives. The principle of k-anonymity is discussed in Section 3. Section 4 portrays the attacks on k-anonymity. The role of cryptography in protecting sensitive data is dealt in Section 5. Section 6 briefs about the homogeneity attack. The background knowledge attack is depicted in Section 7. Section 8 details about Injector mining the background knowledge attack. The concept of t-closeness and existing checking algorithms for (n,t) closeness are discussed in Sections 9 and 10 respectively. The Evolution of Sensitive Data Preservation techniques are discussed in Section 11. Section 12 portrays the sensitive data attack prevention techniques. Techniques to protect trajectory sensitive data are discussed in section 13. Section 14 Concludes the paper and outline the direction for Future Work.

II. DEFINITIONS AND PRIMITIVES

a. Attributes

Let B(a1,a2,…….an) is table with finite no of tuples. The attributes of B are{A1,A2,….An}.The tuples are Ai to Aj and the values are Vi….vj in th e table B. The values that stored in that are each tuple contain data about single person and not to tuples.

b. Quasi- Identifiers

Let V be thespecific table and Quasi identifier for V written sa Qv={name,address,Zip,birthdate,gender}.if we linking the voter list to the medical data {birthdate,ZIP,gender}U Qv.

c. k-Anonymity

Let RT(A1,A2,….An)be a table and QIRT be the Quasi identifier.Rt is said to be k-anonymity if and only if each sequence of values in RT[QIRT] appeare atleast K times in RT[QIRT] .

That is in RT the Quasi identifier data must be apper k times. The K can be 1,2,3…..The K can be said as anonymity of the table.

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 1, Issue 3, November 2014

RACE	Birth	gender	ZIP	Problem
Black	1965	M	0213	shortbreath
Black	1965	M	0213	Shortbreath
Black	1965	M	0214	Hypertension
White	1964	F	0213	Obesity
White	1965	F	0214	Chestpain
White	1967	M	0213	Shortbreath
White	1964	M	0214	chestpain

Fig 1. Microdata Database containing sensitive Information

In the above tables the Black occurs 3 times and white occurs 4 times 1965 occurs 4 times,1967 occurs 1 times,1964 occurs 2 times.The minimum occurancr of the Quasi identifier data is 2.So that is 2 anonymous table.Anonymity is different from what is usual or expected (ie) when we do something , we do not let people know that we are personal who did it and the information. To reduce the disclosure of data, we need to generalize an anonymized table. This anonymized table consist of records that has no. of attributes.

III.K-ANONYMIZATION PRINCIPLE

K-anonymity is a simpler form and are easy to understand. K-anonymity is achieved by anonymising the data before release. Here the explicit identifiers are removed. Though it is not enough as the person may know the quasi-identifier values of some individuals already in the table. The knowledge can be either from the personal knowledge or public. In order to secure both explicit and quasi-identifiers, a generalization method is used, in which all the quasi-identifiers are replaced with less specific values but semantically consistent. As a result more records will have the some values for the quasi-identifier(i.e)K-anonymity requires that each equivalence class atleast K-records. In K-anonymity there are two types of attacks they are homogeneity attack and background knowledge attack .we can discuss the homogeneity attack[16].

IV. ATTACKS ON K-ANONYMITY

a. UNSORTED MATCHING ATTACK AGAINST K-ANONYMITY

If we related the data in the sorting order even if it may be provider with K-anonymity.We can find the data using, that matching with other external sources.So to solve this problem we can provide the data randomly without sorting order.By that we cannot match the in the case of anonymity 2.Otherwise the sensitive data may be matched and leak out.

b. COMPLEMENTARY RELEASE ATTACK AGAINST K-ANONMITY

The subsequent release of two tables which is belonged to a table T.when it be linked, then the data may be disclosed. Consider G,T and GTs are released sub sequently,then the k-anonymity will not hold long time,even if the tuples are changed in random position.When we linking the Quasi identifiers with another attributes in a particular table then the databases may be disclosed.

c. TEMPORAL ATTACK AGAINST K-ANONYMITY

The table GT1 provide k-anonymity at time t=0,form the table PT and some tuples may be added or deleted then the GT2 table provide the k-anonymity and released at the time t1.Then these tables may linked by another attribute of a particular table then that may be reveal the sensitive information.

V. THE ROLE OF CRYPTOGRAPHY IN PROTECTING SENSITIVE DATA

In traditional database security research fully on trustworthy. In assumption possible to the external users (hacker) attack the database. For example health organization database owner and user to interacting with database and also users. So database cannot be fully trusted. This problem can be solved using the role of cryptography. In database security techniques are including access control, information flow control, user authentication, encryption, digital signatures also. And then database security problem and their solution to come up a framework. In that framework occur some relevant security addressed, its point that not previously once. Framework only addressed the new research direction for collaboration of database communities.

A.LIMITATIONS:

Some protocols proposed in the literature of a theoretical communication and can become practical communication bandwidth, computing power can be improved. In real world setting in that assumption may not be fully justified, protocols addressing this issue are even more complex.

B.UNILATERAL SECURITY:

In unilateral security relevant applications, some system must be protected against a malicious outsider often called an attacker. The system is secure has no attacker in system specification. That attacker has no extract the secret information. In that unilateral security is define security as well as define the system specification. For example system capabilities, computing power, bandwidth, etc.

In security to be see internetwork and operating system as well as protection of an organization internal network against hackers for instance by firewalls and intrusion detection technology unilateral security is protection of communication between the two parties against eavesdropper, for example by encryption.

In that required protection of two parties, but eavesdropper not against each other. Database system must protected against outsiders and also against malicious user, but assumed to trust worthy.

C. MULTILATERAL SECURITY

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 1, Issue 3, November 2014

Multilateral Security is an relevant application of on-line transaction require the protection of several parties, each against the potential misbehavior of some other parties. In online transaction where both the customers and the vendors want to be protected against malicious behaviors by the other.

Table 1. Microdata pertaining to Inpatient

	NON SESITIVE ATTRIBUTES			SENSITIVE ATTRIBUTES
	ZIPCODE	AGE	NATIONALITY	DISEASE
1	13053	28	RUSSIAN	CANCER
2	13054	29	JAPANESE	CANCER
3	13068	27	INDIAN	CANCER
4	13068	19	AMERICAN	CANCER
5	14050	31	AMERICAN	HEART DISEASE
6	14050	34	GERMAN	VIRAL INFECTION
7	14068	35	RUSSIAN	CANCER
8	14068	36	INDIAN	VIRAL INFECTION

Table 2. 4-anonymous inpatient microdata

	NON SESITIVE ATTRIBUTES			SENSITIVE ATTRIBUTES
S.No	ZIPCODE	AGE	NATIONALITY	DISEASE
1	130**	<30	*	CANCER
2	130**	<30	*	CANCER
3	130**	<30	*	CANCER
4	130**	<30	*	CANCER
5	140**	3*	*	HEART DISEASE
6	140**	3*	*	VIRAL INFECTION
7	140**	3*	*	CANCER
8	140**	3*	*	VIRAL

Another example of software privacy problem in multilateral security. In software vendor to create the software And provide the user and his functionality, so vendor to give indirectly using the parties, vendors to give parties and parties to give customer, so fully trust the service provider. Another example of multi-lateral security is on-line auctions and e-voting.

	NON SESITIVE ATTRIBUTES			SENSITIVE ATTRIBUTES
	ZIPCODE	AGE	NATIONALITY	DISEASE
1	130**	<30	*	CANCER
2	130**	<30	*	CANCER
3	130**	<30	*	CANCER
4	130**	<30	*	CANCER
5	140**	3*	*	HEART DISEASE
6	140**	3*	*	VIRAL INFECTION
7	140**	3*	*	CANCER
8	140**	3*	*	VIRAL INFECTION

Table 3 Inpatients Microdata

Table 4. A 4-anonymous inpatient microdata

	ZIPCODE	AGE	SEX	DISEASE
1	47665	29	F	VIRAL
2	47602	27	F	CANCER
3	47643	26	M	VIRAL
4	47908	52	M	HEART DISEASE
5	47942	47	F	FLU
6	47932	30	M	HEART DISEASE

D. UNILATERAL DATABASE SECURITY:

In the traditional model of database security, db is assumed to be trustworthy. It suffic es a general system with a state ∑ and set Q of operations .Each query q£Q is specified by a state updates function fq : ∑->∑ and output function gq:∑->β where is the range of all possible replies a query can produce.

E. ACCESS CONTROL

Access control is a most important problem in unilateral security. In that database component checks all the database request and denies user request based on her or his privilege. Access control with developing the policies and languages with specify privileges and then to be implemented the policies. In Access control to subtle has many request queries in the database. In that Access control is a content based meaning or it is based on history of users' previous database.

F. USER AUTHENTICATION AND SECURE COMMUNICATION

The most unilateral problem is an establishing connection between the user and the database. The secure connection to be secret and authenticated in communication. In connection to be implemented by the user. In authenticated to be sub layers stack in the database using public-key – infrastructure(PKI),establishing connection in cryptographic mechanism and protocols.

VI. THE HOMOGENEITY ATTACK

Homogeneity attack means, the way to identify the sensitive attribute of others. For example we consider the two people Anna and Rosita. They are antagonistic

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 1, Issue 3, November 2014

neighbours. They were working in the same company. One day Rosita suffering or some problem physic. Rosita call the ambulance and she admitted in the hospital. Anna saw that Rosita moving in ambulance. Anna don't know that what happen to Rosita. She trying to find what disease for Rosita. so Anna went to hospital and discovers the 4-anonymous table and she look out the current inpatients records that are released by the hospital. Anna saw lots of records.

The records says that admitted patients contain Heart disease, Viral infection, and cancer. But Anna thought that one of the records says about the Rosita. She cant find out in those records. But Anna knows the age of the Rosita because she is neighbor. The age of Rosita is 29-year old Japanese female who lives in zipcode 13068. So Anna easily find out that Rosita lives in 1,2,3,4 in the 4-anonymous inpatients table. That records says that all the patients contain cancer. So Anna concludes that Rosita has cancer. This the one kind of attack in K-anonymity.

VII. THE BACKGROUND KNOWLEDGE ATTACK

Anna has a best friend named Priya who had a ill so she admitted in the same hospital as Rosita. The patient records will be released by the hospital. The fig(1) shows that Anna knows age of Priya is 31-year old Japanese female who currently have a zip code 14050. There is no more information. So she don't know that Priya caught a viral infection or cancer or heart disease. But Anna knows that Japanese have low incidence in the cancer and heart disease. So Anna has concludes that Priya has a viral infection.

In this table we can see that the age of Priya is 31-year old. So the age is 3* so easily identified that Priya has a viral infection. Because the Japanese people have less incidence in cancer and heart disease. This about the background knowledge attack. By overcoming the background knowledge attack they introduced the INJECTOR: mining background knowledge attack[2].

VIII. INJECTOR: MINING THE BACKGROUND KNOWLEDGE ATTACK

In K-anonymity there are two types of attacks they are homogeneity attack and background knowledge attack[2] .we can discuss the background knowledge attack. In the above table says about background knowledge attack. For example Anna has a best friend named Priya who had a ill so she admitted in the same hospital as Rosita. The patient records will be released by the hospital. The Fig.1 shows that Anna knows age of Priya is 31-year old Japanese female who currently have a zip code 14050. There is no more informations. So she don't know that Priya caught a viral infection or cancer or heart disease. But Anna knows that Japanese have low incidence in the cancer and heart disease. So Anna has concludes that Priya has a viral infection. Injector means we are considering the original table that contains all the details. Then we are disclosing the anonymized tables that contains quasi-identifiers (like zip code, age,sex).But for the sensitive attribute we are creating one group id. There we are using id numbers.That table can be disclosure.but the closure table contain the sensitive attributes. By using the group id identify the disease. But the observer will be get confused. This the advantage to overcome background knowledge attack by using INJECTOR: mining background knowledge attack[3].

Table 5 The quasi-identifier table

	ZIPCODE	AGE	SEX	GROUP ID
1	47665	29	F	1
2	47602	27	F	1
3	47643	26	M	1
4	47908	52	M	2
5	47942	47	F	2
6	47932	30	M	2

Table 6 The sensitive attribute table

GROUP ID	DISEASE	COUNT
1	VIRAL DISEASE	2
1	CANCER	1
2	HEART DISEASE	2
2	FLU	1

IX. CONCEPT OF T-CLOSENESS

A positive pregnancy, privacy is measured by the information gain of an observer. Before seeing the released table the observer has think that something happened in the sensitive attribute value of a single person. After seeing the released table the observer may have the details about the sensitive attributes. Here we are going to see about before and after seeing the released table. t-closeness should have the distance between the class and the whole table is no more than a threshold t [15].

X. CHECKING ALGORITHM FOR (N,T) CLOSENESS

INPUT: P is partitioned into partitions $\{p1, p2, \dots pr\}$
OUTPUT: true if (n,t)-closeness is satisfied,false otherwise
STEP1: for every Pi
STEP2: if Pi contains less than n records
STEP3: find = false
STEP4: for every $Q \in parent(p) and\ |Q| \geq n$
STEP5: if $D[Pi, Q] \leq t$, find = true
STEP6: if find == false, return false
The above checking algorithm has three components:
COMPONENT 1:

The first component says how to choose the dimension on which the partition should be done.

COMPONENT2:

The second component is to choose a value for splitting.

COMPONENT3:

The third component says to check partition whether the partition violates the privacy requirement.

To implement the above two components we use existing heuristics[5]. The algorithm is to check if the partitioning will satify the (n,t)-closeness. Here we define

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 1, Issue 3, November 2014

P as a set of tuples. the p is partitioned in to 'r' partitions $\{p1, p2, \ldots . pr\}$ (i.e) $\cup i \{Pi\} = P$ and $pi \cap pj = \emptyset$. then partition P are further partitioned and all the partitions are from the partition tree with P as the root. The parent P denotes the set of partitions on the path from P to the root.in this partitions that contain all the tuples in the table . if the $pi(1 \leq i \leq r)$ contains at least 'n' records , then we can say that pi has the (n,t)-closeness requirements. If the record in $pi(1 \leq i \leq r)$ is less than records , then the algorithm calculate the distance between the pi and each partition in parent(P). if the partition exist is large (contain n records) in parent(P) and which in distance to $pi(D[pi, Q]$ is atmost t, then pi is (n,t)-closeness satisfied. Else pi not satisfy (n,t)-closeness requirements. If all the P is have (n,t)-closeness then the partition g satisfies the (n,t)-closeness requirement.

XI. Evolution of Sensitive Data Preservation Techniques

In (2003) [1] Haoween chan, Perrig.A. in university of California,Berkeley, developed the miniature wireless sensor nodes as part of its smart dust projects. That project establish a self organizing sensor network when dispersed into an environment. the privacy and security issues posed by sensor networks represent a rich field of research problems. The authors says that improving technologies and software may address many of the issues but others will require new supporting technologies.

David A.Maltz, Jibin Zhen,Geoffrey Xie, Hui Zheng,Gisli Hjalmytsson, Albert Greenberg ,Jennifer Rexford in (2004) [2] discussed about anonymizing which is done by removing all information that connects the data to the identity of the originating network ,while still preserving the structure of information that makes the data valuable to networking researchers. Here the authors formulated two methods.Firstly,they have formulated the key issues of the configuration anonymization problem. Secondly,they provided a working solution for configuration anonymization that meets the formulated requirements. Hence it has been validated with a major carrier,earning researchers access to the configuration files for dozens of networks.

RJ Bayardo, R.Agarwal in (2005) [3] said that Hereby the authors present a new approach to explore the space of possible anonymization that develops the data management strategies to reduce the expensive operations such as hashing. The authors shown that the algorithm can produce good anonymization in situations where the input data finding an optimal solution in resoanable time. For their knowledge, this is the first result demonstrating optimal-anonymization of a non-trivial dataset under a general model of the problem.

Jian xu, Wei Wang, Jian pei, Xiaoyuan Wang,Baile Chi, Ada Wai-Chee fu in (2006) [4] studied the problem of utility based anonymization. First, they proposed a simple framework of specifying utility of attributes. That framework covers both numeric data and categorical data. Secondly, they developed two simple efficient local recoding methods for utility based anonymization. Hereby, it results in the utility based method can boost the quality of analysis using the anonymized data.

Gabriel Ghinita, Panagiotis karras, Panos Kalnis, Nikos Mamoulis in (2007) [5], the authors proposed a framework for privacy preservation efficiently that address and cover these defects. At first they focused on one dimensional quasi-identifiers (piece of information) and they developed experience based technique, that finds a solution which is not guaranteed to be optimal(heuristics) to solve the one-dimensional problems in linear time. Finally, they generalized their solutions to multidimensional quasi-identifiers using space mapping techniques.

XII. Sensitive Data Attack Prevention Techniques

Tiancheng Li, NingLui Li in (2008) [6] the author considered and used background knowledge. Their first approach collects knowledge from the data and then it is further used in data anonymization. One important advantage of their approach to that it protects the sata against background knowledge attacks while improving data utility. Then they presented injector framework for data anonymization. Injector collects data to be released and uses then in the anonymization process.They also developed efficient anonymization algorithm to calculate the injected tables that contains background knowledge. Hence, it shows that Injector reduces privacy risks against background knowledge attacks while improving data utility.

TianCheng Li, NingLui Li, Jian Zheng in (2009) [7] portrayed a general framework for analyzing and modeling the adversary's background kno0wledge by using kernel estimation methods. Under this framework, the authors reasoned about privacy using Bayesian inference techniques and proposed skyline (B,t) privacy model. This model allows the data publisher to enforce privacy requirements to protect the data against adversaries. This results in better approach and it shows the effectiveness of their approach in both privacy protection and utility preservation.

Das.S, Egecioglu.O, EL Abbadi.A in (2010) [8] developed a model that preserves properties of the graph which expresses linear functions of the edge weights. These properties forms the foundations of many important graph-theoretic algorithms such as shortest paths, minimum spanning tree etc. hence ,at last as the proof of their concept, they selected the shortest path problem and experimentally evaluated the proposed techniques. They used real social network datasets for their evaluation techniques.

Noman Mohammed, Ruichen, Benjamin C.M.Fung, Philip S.Yu. in (2011 a) [9] the authors proposed the first anonymization algorithm for the non-interactive settings based on the generalization technique. Firstly,their proposed solution generalizes the raw data probabilistically and it adds noise to the guarantee €-differential privacy. for example,they showed that the anonymized data can be used effectively to build a decision tree induction classifier. Hereby,it results that the proposed non-interactive anonymization algorithm is

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 1, Issue 3, November 2014

scalable and performs better than existing solutions for classification analysis.

Jianneng cao, Carminati.B, Ferrari.E, Tan KL in (2011 b) [10] the authors present continuously anonymizing streaming data via adaptive clustering[CASTLE]. It is a cluster-based scheme that anonymizes data. They further shown how CASTLE can be easily extended to handle l-diversity. It is effective and efficient with respect to the quality of the output data.

Aris Gkoulalas-Divanis, Grigorios Loukides in (2011 c) [11] the authors proposed a clustering based framework to anonymizing data while transaction. Their framework provides the basis for designing algorithms that express a larger solution space than existing methods. This method allows publishing data with less information loss and it can satisfy a widerange of privacy requirements.

XIII. TECHNIQUES TO PROTECT TRAJECTORY SENSITIVE DATA

Various approaches have been developed to anonymize clinical data, but they neglect temporal information. Tamersoy.A, Loukides.G, Nergiz.M.E, Saygin.Y,Malin.B in (2012) [12] proposed a novel approach to share patient-specific longitudinal data that offers clear privacy guarantees, while preserving data utility. The authors demonstrated that the proposed approach can generate anonymized data that permit effective biomedical analysis using several patients.

Poulis.G, Skiadopoulos.S, Loukides.G,Gkoulalas-divanis.A. in (2013) [13] paper proposed an approach that overcomes these defects by adapting km-anomity to trajectory data and by using distance based generalization. Their experiments verified that this algorithm preserves data utility and it is fast and scalable.

Burke.M.J, Kayem.A.V.D.M in (2014) [14], the authors made two contributions to facilitate effective and efficient CBCR and crime data mining to address the user privacy concern. Firstly,they proposed a framework for mobile CBCR and secondly,hybrid k-anonymity algorithm is done for preserving crime data. They used hierarchy based generalization algorithm to classify the data to minimize the information loss..

XIV. CONCLUSION

This paper reviewed strategies evolved for protecting sensitive data for the past 10 years. There has been a steep rise in privacy concerns in today's Internet world. There is a definitive need to provide confidentiality as well as preserve privacy of sensitive data. Confidentiality means that data stored in one place unauthorized is difficulty of impossible to access. Usually confidentiality is achieved by be using access policy or used some cryptographic tools. Privacy means the safety provided to the information, without leaking sensitive information. Considering the case of a medical database to join with a research institution. In that case patient's personal health care information and medical information have to be provided for researchers. Hence, in order to provide every patient record privacy, the database needs to be an anonymized version of the patient record then sent to the researchers. Researchers are provided with anonymized database only. The Evolution of Sensitive Data Preservation techniques were discussed. The sensitive data attack prevention techniques were portrayed. Techniques to protect trajectory sensitive data were also intensively discussed.

REFERENCES

[1] Haoween chan, Perrig.A," Security and privacy in sensor networks", published in computer Volume 36, Issue:10, 2003.
[2] David A.Maltz, Jibin Zhen,Geoffrey Xie, Hui Zheng,Gisli Hjalmytsson, Albert Greenberg ,Jennifer Rexford "Structure preserving anonymization of router configuration data", published in 4th ACM SIGCOMM conference on internet measurement, 2004.
[3] RJ Bayardo,R.Agarwal ," Data privacy through optimal k-anonymization" published in 21st International conference,2005.
[4] Jian xu, Wei Wang, Jian pei, Xiaoyuan Wang,Baile Chi, Ada Wai-Chee fu," Utility based anonymization using local recording",published in 12th ACM SIGKDD International conferences on knowledge discovery and data mining, 2006.
[5] Gabriel Ghinita, Panagiotis karras, Panos Kalnis, Nikos Mamoulis," Fast data anonymization with low information loss", published in 33rd International conference on very large databases,2007
[6] Tiancheng Li, NingLui Li," Injector: Mining Background Knowledge for data anonymization",published in 24th International conference on Data Engineering,2008.
[7] TianCheng Li, NingLui Li, Jian Zheng,"Modeling and integrating background knowledge in data anonymization" published in 25th International conference on Data Engineering, 2009.
[8] Das.S, Egecioglu.O, EL Abbadi.A," Anonymizing weighted social network graphs", published in 26th International conference on Data Engineering,2010.
[9] Noman Mohammed, Ruichen, Benjamin C.M.Fung, Philip S.Yu," Differentially private data release for data mining, ACM SIGKDD International conferences on knowledge discovery and data mining,2011 (a).
[10] Jianneng cao, Carminati.B, Ferrari.E, Tan KL," CASTLE: continuously anonymizing data streams", published in dependable and secure computing,(volume:8,issue:3),2011 (b)
[11] Aris Gkoulalas-Divanis, Grigorios Loukides," Privacy –constrained clustering-based transaction data anonymization",published in 4th International workshop on privacy and anonymity in the Information society,2011 (c)
[12] Tamersoy.A, Loukides.G, Nergiz.M.E, Saygin.Y,Malin.B," Anonymization of longitudinal electronic medical records",published in information technology in Biomedicine (volume:16,issue:3), 2012.
[13] Poulis.G, Skiadopoulos.S, Loukides.G,Gkoulalas-divanis.A," Distance-based k^m-anonymization of trajectory data", PUBLISHED IN 14TH International conference on mobile data management,2013.
[14] Burke.M.J, Kayem.A.V.D.M," k-anomity for privacy preserving crime data publishing in resource constrained environments," published in international conference on advanced information networking and application workshop,2014.
[15] Ningui Li, Tiancheng Li and Suresh Venkatasubramanian " Closeness: A new privacy measurefor data publishing", IEEE Transactions on Secure and Dependable Computing, July 2010.
[16] N. Li, T.Li, and S.Venkatsubramanian,"t-closeness : privacy beyond k-anonymity and l-diversity", Proceedings of ICDE pp.106-115,2007.
[17] N. Li, and T.Li, "Injector: Mining background knowledge for data anonymization", Proceedings of ICDE,2008.
[18] A.Machanavajjhala, J.Gehrke, D.Kifer and S.Venkatasubramaniam" l-diversity: privacy beyond k-anonymity", Proceedings of ICDE,p.24,2006.
[19] K. LeFeVer, D.DeWitt and R.Ramakrishnan ," Mondrian Multidimensional K-anonymity", Proceedings of .ICDE, p.25,2006.
[20] P.Samarati, "Protecting respondents privacy in microdata release",IEEE trans,pp1010-1027,dec.2001.
[21] L.Sweeney,"K-anonymity :A model for protecting privacy",pp.557-527, International Journal on Uncertainity, Fuzziness and Knowledge-based Systems, 10(5), 2002.

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 1, Issue 3, November 2014

[22] Balamurugan Shanmugam, Visalakshi Palaniswami, "Modified Partitioning Algorithm for Privacy Preservation in Microdata Publishing with Full Functional Dependencies", Australian Journal of Basic and Applied Sciences, 7(8): pp.316-323, July 2013
[23] Balamurugan Shanmugam, Visalakshi Palaniswami, R.Santhya, R.S.Venkatesh "Strategies for Privacy Preserving Publishing of Functionally Dependent Sensitive Data: A State-of-the-Art-Survey", Australian Journal of Basic and Applied Sciences, 8(15) September 2014.
[24] Charanyaa, S., et. al., , A Survey on Attack Prevention and Handling Strategies in Graph Based Data Anonymization. International Journal of Advanced Research in Computer and Communication Engineering, 2(10): 5722-5728, 2013.
[25] Charanyaa, S., et. al., Certain Investigations on Approaches forProtecting Graph Privacy in Data Anonymization. International Journal of Advanced Research in Computer and Communication Engineering, 1(8): 5722-5728, 2013.
[26] Charanyaa, S., et. al., Proposing a Novel Synergized K-Degree L-Diversity T-Closeness Model for Graph Based Data Anonymization. International Journal of Innovative Research in Computer and Communication Engineering, 2(3): 3554-3561, 2014.
[27] Charanyaa, S., et. al., , Strategies for Knowledge Based Attack Detection in Graphical Data Anonymization. International Journal of Advanced Research in Computer and Communication Engineering, 3(2): 5722-5728, 2014.
[28] Charanyaa, S., et. al., Term Frequency Based Sequence Generation Algorithm for Graph Based Data Anonymization International Journal of Innovative Research in Computer and Communication Engineering, 2(2): 3033-3040, 2014.
[29] V.M.Prabhakaran, Prof.S.Balamurugan, S.Charanyaa," Certain Investigations on Strategies for Protecting Medical Data in Cloud", International Journal of Innovative Research in Computer and Communication Engineering Vol 2, Issue 10, October 2014
[30] V.M.Prabhakaran, Prof.S.Balamurugan, S.Charanyaa," Investigations on Remote Virtual Machine to Secure Lifetime PHR in Cloud ", International Journal of Innovative Research in Computer and Communication Engineering Vol 2, Issue 10, October 2014
[31] V.M.Prabhakaran, Prof.S.Balamurugan, S.Charanyaa," Privacy Preserving Personal Health Care Data in Cloud" , International Advanced Research Journal in Science, Engineering and Technology Vol 1, Issue 2, October 2014
[32] P.Andrew, J.Anish Kumar, R.Santhya, Prof.S.Balamurugan, S.Charanyaa, "Investigations on Evolution of Strategies to Preserve Privacy of Moving Data Objects" International Journal of Innovative Research in Computer and Communication Engineering, 2(2): 3033-3040, 2014.
[33] P.Andrew, J.Anish Kumar, R.Santhya, Prof.S.Balamurugan, S.Charanyaa, " Certain Investigations on Securing Moving Data Objects" International Journal of Innovative Research in Computer and Communication Engineering, 2(2): 3033-3040, 2014.
[34] P.Andrew, J.Anish Kumar, R.Santhya, Prof.S.Balamurugan, S.Charanyaa, " Survey on Approaches Developed for Preserving Privacy of Data Objects" International Advanced Research Journal in Science, Engineering and Technology Vol 1, Issue 2, October 2014
[35] S.Jeevitha, R.Santhya, Prof.S.Balamurugan, S.Charanyaa, " Privacy Preserving Personal Health Care Data in Cloud" International Advanced Research Journal in Science, Engineering and Technology Vol 1, Issue 2, October 2014
[36] S.Balamurugan, S.Charanyaa, "Principles of Social Network Data Security" LAP Verlag, Germany, ISBN: 978-3-659-61207-7, 2014.

BIOGRAPHIES

K.Deepika, P.Andrew and R.Santhya are currently pursuing their B.Tech. degree in Information Technology at Kalaignar Karunanidhi Institute of Technology, Coimbatore, Tamil Nadu, India. Their areas of research interests include Network Security, Cloud Computing and Database Security.

Prof.S.Balamurugan obtained his B.Tech degree in Information Technology from P.S.G. College of Technology, Coimbatore, Tamil Nadu, India and M.Tech degree in Information Technology from Anna University, Tamil Nadu, India respectively. He is currently working towards his PhD degree in Information Technology at P.S.G. College of Technology, Tamil Nadu, India. At present he holds to his credit **50 papers International Journals and IEEE/ Elsevier International Conferences.** He is currently working as Assistant Professor in the Department of Information Technology, Kalaignar Karunanidhi Institute of Technology, Coimbatore, Tamil Nadu, India affiliated to Anna University TamilNadu, India. He is **State Rank holder** in schooling. He was **University First Rank holder** M.Tech. Semester Examinations at Anna University, Tamilnadu, India. He served as a Joint Secretary of IT Association, Department of Information Technology, PSG College of Technology, Coimbatore, Tamilnadu, India. He is the **recipient of gold medal and certificate of merit** for best journal publication by his host institution **consecutively for 3 years**. Some of his professional activities include invited Session Chair Person for two Conferences. He has guided 12 B.Tech projects and 2 M.Tech. projects. He has won a best paper award in International Conference. His areas of research interest accumulate in the areas of Data Privacy, Database Security, Object Modeling Techniques, and Cloud Computing. He is a life member of ISTE,CSI. **He has authored a chapter in an International Book "Information Processing" published by I.K. International Publishing House Pvt. Ltd, New Delhi, India, 978-81-906942-4-7. He is the author of book titled "Principles of Social Network Data Security", ISBN: 978-3-659-61207-7.**

S.Charanyaa obtained her **B.Tech** degree in Information Technology and her **M.Tech** degree in Information Technology from Anna University Chennai, Tamil Nadu, India. She was **gold medalist** in her B.Tech. degree program. She has to her credit **12 publications in various International Journals and Conferences**. Some of her outstanding achievements at school level include **School First Rank holder** in **10th and 12th grade**. She was working as Software Engineer at Larsen & Turbo Infotech, Chennai for 3 years where she got promoted as Senior Software Engineer and worked for another 2 years. She worked at different verticals and worked at many places including Denmark, Amsterdam handling versatile clients. She is also the recipient of **best team player award for the year 2012 by L&T**. Her areas of research interest accumulate in the areas of Database Security, Privacy Preserving Database, Object Modeling Techniques, and Cloud Computing. **She is the author of book titled "Principles of Social Network Data Security", ISBN: 978-3-659-61207-7.**