International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org, editorijaiem@gmail.com
Volume 2, Issue 5, May 2013 ISSN 2319 - 4847

Critical Security Threats in Online Information Systems

Jayanta Mondal[1], G.K. Panda[2]

[1]Scholar, M.Tech., Berhampur University,

[2] Faculty, MITS, Rayagada, Odisha, India

ABSTRACT

Advances in technology have made it possible to collect data about individuals and the connections between them, such as email correspondence and friendships. Agencies and researchers who have collected such data often have a compelling interest in allowing others to analyze the data. However, in many cases the data describes relationships that are private (e.g., email correspondence) and sharing the data in full can result in unacceptable disclosures. Today privacy and security issues in online information systems and social networks in particular have become a critical issue. We discuss some of the probable privacy and security issues in online social networks and present security mechanisms along with anonymisation techniques for social network services in particular.

Keywords: Information Security, Social Networks, Privacy Preservation, Anonymisation

1. INTRODUCTION

Information security can be viewed through wiki as the set of methodologies for protecting information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction satisfying three basic principles like Integrity, Confidentiality and Availability. The first standard is enlightened on the mechanisms to guard against improper modification or destruction of information ensuring non-repudiation and authenticity. The second standard focuses on policies to preserve authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; where the last standard ensures timely and reliable access to and use of information.

In this digital competing market, information is evolving as a critical asset in the operation of any business. The data being collected by a company and shared is the very definition of the relationships with its vendors and customers, as well as the foundation for its internal operations and business processes. Protecting the information is as important as protecting cash or valuables and needs utmost care and planning.

Information security is about safeguarding these critical information assets, ensuring the integrity of the data on which decisions and transactions are relied, its availability for business operations and its confidentiality for both the company and its customers. It is a process of putting policies, procedures and technical mechanisms to protect, detect and correct problems before they threaten the business. Anything that threatens one's information systems does threaten to whole business. If confidential information about customers, finances or new product of a company line falls into the hands of a competitor, one can lose competitive advantage at best or suffer significant market losses at worst. Thus, it needs attention to manage the risk proactively and to away from innumerable complications. Here we discuss some of the initiations to protect privacy of information in terms of international acts and legal laws.

2. INFORMATION SECURITY

2.1 International Acts and Laws

Relevant U.S. Laws - General Computer Crime Laws: The Computer Fraud and Abuse Act of 1986 is the cornerstone of many computer-related federal laws and enforcement efforts. It was amended in October 1996 with the National Information Infrastructure Protection Act of 1996, which modified several sections of the CFA and increased the penalties for selected crimes.

The USA Patriot Act of 2001 modified a wide range of existing laws to provide law enforcement agencies with broader latitude of actions to combat terrorism-related activities. *The Communication Act of 1934* was revised by the Telecommunications Deregulation and Competition Act of 1996, which attempts to modernize the archaic terminology of the older act. These much-needed updates of terminology were included as part of the *Communications Decency Act*

(CDA). The CDA was immediately ensnared in a thorny legal debate over the attempt to define indecency, and ultimately rejected by the Supreme Court. Another key law that is of critical importance for the information security professions is the *Computer Security Act* of 1987. It was one of the first attempts to protect federal computer systems by establishing minimum acceptable security practices. The National Bureau of Standards, in cooperation with the National Security Agency, became responsible for developing these security standards and guidelines.

Information and privacy compromises make the news today in public domains; a security breach that puts one's name in the headlines cannot only damage the reputation and credit rating, but can leave exposed to lawsuits and even bankruptcy. Increasingly, government is responding to concerns about information privacy and security, creating new regulations about how customer and financial information should be protected. Failure to comply with these regulations can result in punitive fines, lawsuits and even personal liability for breaches.

3. PRIVACY AND SECURITY IN SOCIAL NETRORK

3.1 Social Network

Social network is termed as a social structure made up of set of actors (such as individuals or organizations) and the dyadic ties between these actors. Social networking service is evolving as an online service, platform, or site that focuses on facilitating the building of social networks among people who, for example, share interests, activities, backgrounds, or real-life connections. Internet based online patterns of friendships between individuals, business relationships between companies, sharing of information in intellectual, academic and bureaucratic communities across globe, advancement of blogs and intermarriages between families are all examples of evolving networks lead into a new dimension of research and popularly of Online Social networking.

Figure 1 Examples of Social Networks

Social Networks (SNs) have significant business value due to their marketing policies and applications. On SNs people profile themselves for free and voluntarily disclose detailed maps of their social relationships. In 2005, MySpace was sold for a price that corresponded approximately to US$ 35 per user profile [19]. In 2006, Facebook sources suggested a valuation for their network of US$ 2 billion [20] (which would translate to US$ 286 per user profile) and by March 2011, this figure had risen to US$ 76.4 billion [21].

The success of any SN depends on the number of users it attracts which makes an attention to the SN providers to prioritize on the design methodology and behavior patterns among the users and their connections. As with every fast-growing technology, security and privacy have not been the first priority in the development of SNs. As a result significant privacy and security risks have also emerged.

3.2 Privacy in Social Networks

Social networking services range from social-interaction centered sites such as Facebook or MySpace to information-dissemination-centric services such as Twitter or Google Buzz to social interaction features like Flickr or Amazon and variations have gained more popularity in recent years. Because of its large user base, and large amount of information, they become a potential channel for attackers to exploit. Many social networking sites try to prevent those exploitations, but many attackers are still able to overcome those security countermeasures by using different techniques. Social network users may not be aware of such threats.

Most social network users share a large amount of their private information in their social network space. This information ranges from demographic information, contact information, comments, images, videos, etc. Many users publish their information publicly without careful consideration. Hence, social networks have become a large pool of sensitive data. Moreover, social network users tend to have a high level of trust toward other social network users. They tend to accept friend requests easily, and trust items that friends send to them.

Cyber criminals exploit sensitive data and chain of connection mostly through social engineering and reverse social engineering (RSE).The goal of these two methods is to obtain user's context-information i.e. information that is related or meaningful to users. Both methods are being used prior to other attacks such as phishing, spamming, and malware attack. In social engineering, attackers approach user's accounts and extract user's context-information then use this information to increase successfulness of their attacks. On the other hand, in the RSE method, attackers will not directly approach users. They will try to trick users to initiate a contact with them or influence users to perform some actions.

There are three methods to perform RSE. The first one is recommendation-based RSE. This method makes use of friend recommendation feature to introduce attackers to the victims. The second is demographic-based RSE. This method is also based on friend recommendation feature that exploits victim's demographic information such as user's locations and interests. The last method is visitor-tracking based RSE. This method is based on the visitor tracking feature of some social networks websites. The feature allows users to find out who have viewed their profiles. Attackers can use this feature to make victims notice them, and visit their profiles.

4. SECURITY ISSUES IN SOCIAL NETWORK

In this section we present different privacy and security issues in online social networks. The issues include public identity, identity theft issues, spam issues, malware issues, and physical threats issues.

4.1 Users' Anonymity

In many social networking sites, users use their real name to represent their accounts. So, their identity is exposed publicly to other social network users, as well as everyone else in the online world. Also, social network user's account can be indexed by search engine and usually appeared in the top rank of the search results. In this case, if attackers know the name of the victims, they can easily search for victim's profile, or they can search through social networking sites to obtain new victims. Apart from the simple use of real name as account name, there are also other techniques that can be used to expose social network user's anonymity.

4.2 Identity Theft

Identity theft is an act of stealing someone's identity or sensitive information, and then pretending to be that person, or using that identity in a malicious way. Social networks are promising targets that attract attackers since they contain a huge number of available user's information. ***Profile cloning*** is one of the techniques of this type where attackers take advantage of trust among connected links and dominates in the periphery where people are not careful when they accept friend requests. ***Existing profile cloning*** and ***Cross-Site profile cloning*** are two extensions to this. ***Social phishing*** is also another technique and used to steal social network user's identity.

4.3 Profile and Personal Information Leakage

Social network user's profiles mostly contain sensitive information such as user's full name, contact information, relationship status, date of birth, previous and current work and education background which attract attackers. Therefore, the main issue of user's profile is the leakage of profile and personal information. Sources of users' profile leakage are Leakage of information through poor privacy settings, Leakage of information to 3 rd party application, and Leakage of information to 3 rd party domain.

4.4 Spam Attacks in Social Networks

Spam attacks in traditional electronic mailing systems are becoming inefficient. Most of the spam are filtered through the service provider (yahoo, google) and do not reach the victim. Even if the spam reaches the victims, there is a high chance that victims just delete them, since most victims are well aware of spam. However, in the public domains like social network systems, the new way of making spam attack is high.

In most of the social networks, spam comes in the form of wall post, news feed and messages. This kind of spam is more effective than the traditional email spam since users spend more time on social networking sites than they do on

checking their email. Spam attacks in social networks usually pass through advertisements and hyperlinks in hope that victims would click through that link. These links may lead to harmful phishing sites or malware sites.

Email is a common target of online attacks and Spam has been a problem for email's users for a long time. Even though social networking sites allow users to keep their email private, attackers can still use user's information such as user's first name and last name to guess for their email address.

Attackers obtain valid emails from social networks easily through the friend finding feature which allows registered users to search for friends by specifying email addresses. Attackers exploit this feature by using a large list of randomly generated email address to retrieve valid emails. If the email exists, the results show the corresponding accounts. There are 2 main types of spam. Broadcast Spam and Context-Aware spam are two approaches of spam attacks in social networks. In Broadcast Spam, attackers broadcast emails to all email addresses in their lists. The contents on the email are not specific to any victims. Hence, victims can easily recognize them as spam, and delete them. In Context-Aware Spam, attackers aggregate context information from a user's shared information such as date of birth, wall post, and news feeds, or relationship to social networks friends to generate email spam that matches user's preferences. The chance of success of context-aware spam attack is more compared to the broadcast spam attack.

For example, if attackers know that A is B's friend, then an attacker can send a fraud email saying that A posted something on B wall, and provide a fake link for B to follow to see that post. Another case is if attackers also know B's birthday, then they can send a fake online birthday card to B by saying that the card is sent by A.

4.5 Malware Attacks in Social networks

The intention of attacker is to design hostile or intrusive software, is termed as Malware, which can disrupt computer operation, gather sensitive information or gain access to private computer systems. The chance of spreading malware is phenomenal with the rapid growth of interconnections in social networks. To date, many social network websites are still lacking of mechanisms to determine whether URLs or embedded links are malicious or not. Hence, attackers can exploit this flaw. Followings are some techniques used by attackers.

***Fake Profile*:** Attackers create a fake profile to lure or tempt other users of social network to connect with them and to view their profile. The fake profile can be in the form of for example, a celebrity's profile that attracts victims to contact them.

***Social Network API*:** Third party applications can be the source of social network user's information leakage. In this case, these applications are also potential sources of malware infection since all users can easily access the application. In user's view, these applications may look authentic, and seem to operate as if it should be, but inside it might hide a malicious link that takes users to malicious domain, and spreads malware to users.

APIs for OpenSocial (Source: IBM Almaden Research Center http://www.almaden.ibm.com/cs/projects/iis/ppn/**)**

double getPrivacyScore (userID, key)

• Description: Gets the user's privacy score, which is calculated by the native Implementation. The key specifies the mathematical model, i.e., Naïve or IRT.

double getPrivacyScore (userID)

• Description: Gets the user's privacy score

int getPrivacySetting (userID, profileItemID)

• Description: Gets user's privacy setting for the profile item

Boolean setPrivacySetting (userID, profileItemID, PrivacySetting)

• Description: Sets the user's privacy setting for the profile item

profileItemID can be chosen from opensocial.Person.Field, opensocial.Address.Field, opensocial.Email.Field, opensocial.Name.Field, opensocial.Organization.Field, opensocial.Phone.Field, etc.

***Drive-by Download Attack*:** This type of attack uses advertisement as a medium to spread malware across social networks. Attackers post malicious advertisement on social network user's wall or message board. When users click on adds, they will be redirected to the malicious websites that then will prompt victims to download malicious code such as Java or ActiveX content to their browser.

Shortened and Hidden Links: URL shortening has been a popular method that allows people to reduce the size of their URLs since many URLs are too long. People can easily access this type of service. What they have to do is to submit the original URL. The service then will generate the shortened version of the URL that will redirect to the original URL when being used. According to the Symantec Cooperation Survey on malicious shortened URLs on social networking sites, *"65% of malicious URLs on social networks were shortened URLs, and 88% of those URLs were clicked by social network users"*.

***Cross-Site Scripting Attack*:** Cross-site scripting (XSS) is one of the web application vulnerabilities that run on a web browser. Cross-site scripting feeds JavaScript to victim's browser. An attacker can write dynamic HTML code to make the web browser send victims cookies to attacker's server.

***Clickjacking*:** Clickjacking is a technique which attackers trick victims into clicking on a button or an item. Then, the hidden code will be triggered to perform some malicious action.

5. SECURITY MECHANISMS IN SOCIAL NETWORKS

Many users are not careful about what they expose on their social network space and not aware of the size of the audience accessing their content. The sense of intimacy created by being among virtual friends often leads to inappropriate or damaging disclosures. In this section we discuss some of the security mechanisms and strategies to prevent and improve privacy and security in social networks without compromising the benefits of information sharing.

Most of the recent works have focused on managing balance between privacy and utility in data publishing, but applicable only to some limited type of datasets. Some efforts in this direction are the k-anonymity [9, 10, 11, 12] and its many variants, its extensions *l*-diversity [8] and *t*-closeness [5], which are data perturbation techniques designed for tabular micro-data, which typically consists of a table of records, each of which describes an entity. These algorithms are not suitable to tackle the anonymisation problem of social networks. A common assumption underlying all these techniques is that the records are independent and can be anonymised (more or less) independently. In contrast, social network data forms a graph of relationships between entities. Existing tabular perturbation techniques are not equipped to operate over graphs and they will tend to ignore and destroy important structural properties. Likewise, graph structure and background knowledge combine to threaten privacy in many new ways.

Privacy of knowledge may be leaked if a social network is released improperly to public. We have experienced the fact that when an individual, organization or a social group innovates successfully, the knowledge on which that progress is based becomes visible, at least partially, in the immediate neighborhood. As time goes on, such progress is understood and copied.

As a first step to hide information, the released social network has to go through the anonymisation procedure which replaces social entity names with meaningless unique identifiers [11]. Although this kind of anonymisation may still leak a lot of information. Protection against the threat of re-identification presents novel challenges for graph structured data. In tabular data, identified attributes can be generalized, suppressed or randomized easily, and the effects are largely restricted to the individual entities affected. It is much harder to generalize or perturb the structure around a node in a graph, and the impact of doing so can spread across the graph.

In order to ensure anonymity we require that the adversary has a minimum level of uncertainty about the re-identification of any node in the vertex set. The condition implies that there are at least k candidate nodes for any node x in the original data, and furthermore, all the candidates are equally likely. This is a generalization of basic k-anonymity in the sense that, if the probability distribution over candidates is uniform, this definition simply requires at least k candidates. Graph anonymisation by edge perturbation results in a more complex probability distribution over candidates, for which this general definition is required.

Hay et al. [4] presented a framework for assessing the privacy risk of sharing anonymised network data. They modeled the adversaries' background knowledge as vertex requirement structural queries and proposed a privacy requirement k-candidate anonymity which is similar to k-anonymity in tabular data.

Thomson and Yao [13] have presented two clustering algorithms for clustering undirected graphs that group similar graph nodes into clusters with a minimum size constraint. Also, they have developed an inter-cluster matching method for anonymising social networks by strategically adding and removing edges based on the social role of the nodes.

Zhou and Pei proposed an anonymisation technique for social networks to prevent the neighborhood attacks [18]. They have anonymised the social network using depth-first search (DFS for short) codes and minimum DFS codes.

This approach gives a simpler solution but is limited to the case that the adversary has information about the immediate neighbor only. It can protect against 1-neighbourhood attack only.

Recently, Tripathy and Panda [15] et al introduced an algorithm for graph isomorphism based on adjacency matrix instead of their approach using DFS technique [18]. To this effect they introduced a subgraph isomorphism algorithm by improving the brute force subgraph isomorphism algorithm. Also, the algorithm protects the identity of the nodes of the social network even if the adversary has information not just about the immediate neighbors, but also about the nodes within finite number of hops from the target node. The algorithm provides higher security level at a lower time complexity.

Suppression and generalization are the two common approaches to anonymise databases. In suppression a value is not released at all. In the process of generalization, the quasi-identifier (identifier can be linked) values are replaced by values which are less specific but semantically consistent. Also, the notion of generalization is enhanced by imposing on each value generalization hierarchy a new maximal element, atop old maximal element. As a result of generalization, more records have the same set of quasi-identifier values. Such a set of records are said to form a cluster or sometimes an equivalence class.

The large amount of information easily accessible today, together with the increased computational power available to the attackers, makes linking attacks a serious problem [4]. The information disclosure has been identified to be of two types. These are; identity disclosure and attribute disclosure. In identity disclosure an individual is linked to a tuple in the database and so the information available is supposed to belong to that individual. Attribute disclosure occurs when additional information about an individual is obtained, which were not present at the time of release of the data table. It is worth noting that identity disclosure leads to attribute disclosure. However, attribute disclosure may not necessarily need identity disclosure.

To handle linking disclosure while preserving the integrity of the released data, Samarati and Sweeney proposed the concept of k-anonymity [9]. In this approach, data privacy is guaranteed by ensuring that any record in the released data is indistinguishable from at least (k-1) other records with respect a set of attributes called the quasi-identifiers. In later years it was further expanded by Sweeney [11,12] to the context of table releases. While *k*-anonymity protects against identity disclosure, it does not provide sufficient protection against attribute disclosure. Although the idea of k-anonymity is conceptually straightforward, the computational complexity of finding an optimal solution for the k-anonymity problem has been shown to be NP-hard, even when one considers only the technique of suppression of values [1, 3]. In order to obtain k-anonymity, several algorithms have been introduced in recent times [1, 2, 5, 6, 10, 11, 12]. The basic idea in most of these algorithms is that k-anonymisation problem can be viewed as a clustering problem. Intuitively, the k-anonymity requirement can be naturally transformed into a clustering problem where we want to find a set of clusters, each of which contains at least k records. In order to maximize data quality, we also want the records in a cluster to be similar to each other as much as possible. This ensures that less distortion is required when the records in a cluster are modified to have the same quasi-identifier value. Some significant contributions in the devise of k-anonymisation algorithms are as follows.

The k-anonymity requirement is typically enforced through generalization, where real values are replaced with “less specific but semantically consistent values [9]”. Given a domain, there are various ways to generalize the values in the domain. Typically numerical values are generalized into intervals and categorical values are generalised into a set of distinct values or a single value that represents such a set. Many times a non-overlapping generalisation hierarchy is first defined for each attribute of quasi-identifier. Then an algorithm tries to find an optimal (or good) solution which is allowed by such generalization hierarchies. Although this leads to much more flexible generalization, possible generalizations are still limited by the imposed generalization hierarchies.

Some schemes those do not rely on generalization hierarchies have been proposed. For instance, LeFevre et al transform the k-anonymity problem into a partitioning problem. Although shown to be efficient, these approaches also have a disadvantage that it requires a total order for each attribute domain. This makes it impractical in most cases involving categorical data which have no meaningful order.

Transforming a k-anonymity problem into a clustering problem, called the k-member clustering problem, Byun et al [2] developed an algorithm. De-identifying data through common formulations of k-anonymity is unfortunately NP-hard if one wishes to guarantee an optimal anonymisation [2]. Algorithms that are suitable for use in practice typically employ greedy methods or incomplete stochastic search Li et al [5] and do not provide any guarantees on the resulting anonymisation. Bayardo and Agrawal [1] have developed an algorithm which they have shown to be both practical and

guarantees on solution quality. It has been shown by them that most of the other algorithms satisfy either of the two requirements but not both.

In Lin et al [6], a new clustering-based method known as OKA (One pass K- means Algorithm) is proposed for k-anonymization which has advantages over some of the preceding algorithms proposed by Byun et al [2], Loukides and Shao [7] and Chiu and Tsai [3]. The OKA algorithm has two phases. It first clusters the data tuples and then in the adjustment stage makes up the sizes of the clusters to have a minimum of k elements each.

Background knowledge and homogeneity attacks are the two attacks where a k anonymous table may disclose the sensitive information. Homogeneity attack is a result of the fact that k-anonymity can create groups that leak information due to lack of diversity in the sensitive attribute. Also, k-anonymity does not protect against attacks based on prior knowledge of the adversary which results in background knowledge attack. As a solution to these problems and provide greater privacy the notion of *l*-diversity [5] was proposed. In fact *l*-diversity provides privacy even when the data publisher does not know what kind of knowledge the adversary possesses. The main idea behind *l*-diversity is the requirement that the values of the sensitive attributes are well represented in each group. The simplest expression of the property of "well represented" can be having at least *l* distinct values for the sensitive values in each group, which is called distinct *l*-diversity. There two other types of *l*-diversities which shall be introduced later. If a table has *l*-diversity then both the above two attacks can be handled.

Panda et al [14, 16, 17] proposed first ever algorithm to achieve *l*-diversity which satisfies distinct *l*-diversity. Uncertainty has become an integral part of modern day databases. Several data clustering algorithms exist, which handle uncertainty. A group of such algorithms use rough set as the basis for handling uncertainty and achieves *l*-diversity in addition to handling uncertainty and also takes care of hybrid data.

6. CONCLUSION

Social networking sites have become a potential target for attackers due to the availability of sensitive information, as well as its large user base. Therefore, privacy and security issues in online social networks are increasing.

Privacy issue is one of the main concerns, since many social network user are not careful about what they expose on their social network space. The second issue is identity theft; attackers make use of social networks account to steal victim's identities. The third is the spam issue. Attackers make use of social networks to increase spam click through rate, which is more effective than the traditional email spam. The forth is the malware issue. Attackers use social networks as a channel to spread malware, since it can spread very fast through connectivity among users. Social networking sites are always facing new kind of malware. Lastly, physical threats, which are the most harmful issues, were addressed. Because of some of the social network features such as location-based service, it is easier for criminal to track and approach victims. We presented the related work of anonymisation techniques done in the field of social network. A further approach of anonymisation technique and its practical implementation on the field of dataset may lead us to a fruitful result for privacy preservation.

References

[1] Atanassov, K.T.: Intuitionistic Fuzzy Sets, *Fuzzy Sets and Systems*, 20, (1986), pp.87 – 96.
[2] C. Dwork: Differential privacy, *Automata, languages and programming*, 2006, pp. 1–12.
[3] Christopher B: A Tutorial on Support Vector Machines for Pattern Recognition, *Intl. Journal, Data Mining and Knowledge Discovery*, 2(2)(1998).
[4] Holland, J. H., Holyoak, K. J., Nisbett, R. E.: Induction Process of Inference, Learning and Discovery, *Cambridge, MA: The MIT Press.*
[5] Liang, J.Y, Shi, Z.Z., Li, D. Y. and Wierman, M. J.: The information entropy, rough entropy and knowledge granulation in incomplete information system, *Intl. Journal of general systems*, vol. 35(6), (2006), pp.641 – 654.
[6] Loukides, G. and Shao, J.: Capturing data usefulness and privacy protection in k-anonymisation, 2007 ACM symposium on Applied Computing, 2007.
[7] M. Just and D. Aspinall,: Personal choice and challenge questions: a security and usability assessment, *Proceedings of the 5th Symposium on Usable Privacy and Security*, 2009, pp. 1-11.
[8] Mathieu, R. and Gibson, J.: A Methodology for large scale R&D planning based on cluster analysis, *IEEE Transactions on Engineering Management* (2004), 40 (3), pp. 283–292.
[9] Slowinski R. and Vanderpooten D., Similarity Relation as a Basis for Rough Approximations, *P.P. Wang, Editor, Advances in Machine Intelligence & Soft-Computing*, Vol. IV, Duke University Press, Durham, NC(1997), pp. 17-33.

[10] Suykens, J.A.K., and Vandewalle, J.: Least Squares Support Vector Machine Classifiers. *Neural Processing Letters*, Vol.9, No.3 (1999).
[11] Thompson, B. and Yao, D.: The Union-split Algorithm and Cluster-Based Anonymization of Social Networks, *ASIACCS'09*, Sydney, NSW, Australia March, 2009, pp. 10-12.
[12] Tripathy B. K.,: Rough sets on Intuitionistic Fuzzy Approximation Spaces, Proceedings of *3rd Intl. IEEE Conference on Intelligent Systems (IS06)*, London, Sept. 4-6(2006), pp.776-779.
[13] Tripathy, B. K.: An Analysis of Approximate Equalities based on Rough Set Theory, *Intl. Journal of Advanced Science and Technology, Vol. 31*, (2011),pp. 23-36.
[14] Tripathy, B. K., Kumaran, K., and Panda, G. K.,: An Improved *l*–diversity Anonymisation Algorithm, *5th Intl. Conf. on Information Processing, Springer Verlag, Communications in Computer and Information Sciences(CCIS)*, 157, (2011), pp. 81-86.
[15] Tripathy, B. K. and Panda, G. K. : A New Approach to Manage Security Against Neighbourhood Attacks in Social Networks, *The Intl. Conf. on Advances in Social Networks Analysis and Mining, ASONAM 2010,University of Southern Denmark, Denmark, 2010*, IEEE Computer Society, (2010),pp. 264-269.
[16] Tripathy, B. K., Panda, G. K. and Kumaran, K.: A Fast *l*-diversity Anonymisation Algorithm, *Proc. of the third Intl. Conf. on Computer Modeling and Simulation-ICCMS 2011*, Mumbai, Jan, 2011,(2) pp.648-652.
[17] Tripathy, B. K., Panda, G. K., and Kumaran, K.: A Rough Set Based Efficient *l*-diversity Algorithm, In: Intl. Journal of Advances in Applied Science Research, Pelagia Research Library, Vol:2, Issue:3, May(2011), pp.302-313.
[18] Zhu, W. and Wang, F. Y.: Relationships among Three Types of Covering Rough Sets, *IEEE GrC 2006, IEEE Press, Los Alamitos*, May (2006) pp. 43-48.
[19] BBC News, 19 July, 2005. News Corp in $580m Internet buy , http://news.bbc.co.uk/2/hi/ business/4695495.stm
[20] Ian Sefferman. By the Numbers – Is Facebook worth $2 Billion?, 2006, www.iseff.com/ 2006/04/ by- numbers-is-facebook-worth-2-billion.html
[21] BBC - dot.Rory: Russian bank: Facebook worth $76.4bn www.bbc.co.uk/.../2011/.../russian_bank_facebook_worth_..

AUTHOR

Jayanta Mondal received his B.Tech degree in Information Technology from Siliguri Institute of Technology in 2011 and currently perusing M.Tech in M.I.T.S., Rayagada under Berhampur University Odisha, India.