DDOS ATTACK DETECTION USING DATA MINING TECHNIQUE

[1]**Shreshtha Jha,**
B Tech Final Year, Department of computer Science,
VIT University, Vellore

ABSTRACT

Cyber Crime is a computerized wrongdoing relating to something that ought to be conceivable on the web and isn't lawful. Bad behavior related to something that is done unlawfully or without endorsement. Every last one of those infringements that are done on the web to get to secured information or endorsement rights is named as "Cyber Crime". All around the computerized bad behavior anticipation is spread transversely finished generously. Data figuring underlines the extraction of data from databases and diverse cases can be done up for surmising connection rules. Notwithstanding the way that Data preparing is over the long haul grabbing an all the all the more encompassing degree in different districts, its examination has made awesome importance in Cyber Crimes.

Index Terms:Cyber Attack, Cyber Crimes in Data mining, Data Analysis, Machine Learning, DDOS, IP based Computing, I-Security, Thread Detection

INTRODUCTION

Web's brisk headway examines uncontrolled advanced bad behavior information happening in the web. In this paper the web data is bankrupt down using the data mining techniques with the elucidated contemplate on gathering and packing. The request technique is enhanced the circumstance portraying sort of bad behavior activity performed on the web. The bundling system is enhanced the circumstance solidifying data challenge into social affairs. The circumstance create removes the site page properties and relations and besides recreates the prelude for bad behavior mining using the IP.Data computing depicts various computing techniques which uses more PCs associated through system (Internet). By and large, the information registering shares figuring assets as opposed to using the nearby servers or individual gadgets for performing application. The fundamental stress in associations considering is Security that is charged Data choice especially open Data gathering. The data authority centers in the Public cloud share their chief system of hardware among armed force customers, in light of the way that general society cloud is known as a multi-tenant condition. The multi-occupant condition requires plenteous stopping between reliable figure resources. At the same time getting the opportunity to individuals when all is said in done cloud data and figuring the advantages are ensured with account login affirmations. Every last one of the affiliations are taken after with the complex administrative obligations and organization measures that are up 'til now reluctant to influence circumstances of data or workloads when all is said in done society to cloud roused by a distrustful dread of power outages, incident or theft. All things considered, this restriction is blurring, as coherent confinement has demonstrated dependable, and the expansion of information encryption and different character and access administration apparatuses includes enhanced security inside the general population cloud. The advancement, inescapability and enhancing capacity energy of PC innovation have expanded information accumulation storage room and furthermore the information control. Expanded information investigation is in a roundabout way enlarged by performing programmed information handling with expanded informational indexes size and unpredictability. The basic stress in associations considering is Security that is assumed Data assignment especially open Data gathering.The information specialist organizations in the Public cloud share their key foundation of equipment among trusted army clients, in enlightenment of the fact that general society cloud is known as a multi-inhabitant condition. The multi-occupant condition requires plenteous stopping between coherent register assets. All the while getting to the general population cloud information and figuring the assets are watched with account login accreditations. Each of the firmsfollowsthe complex administrative commitments and administration principles that are as yet hesitant to make arrangements of information or workloads in the general population cloud inspired by a paranoid fear of blackouts, misfortune or robbery. The principle legitimateexplanation behind performing information digging which is also known as data miningprocess is for examining, gathering and watching the conduct. Deceitful exchanges are effortlessly recognized utilizing the Data mining procedures which can be successfully group and distinguish utilizing the order calculation. The basic point is to propose a secured application which perceives progressed unlawful conduct and actives. The proposed structure is incorporated with two-stage computerized bad behavior area systems and has various stages procedure to experience to improve the security of the system. The primary stage includes gathering the information and examining the information. The second stage includes developing IP based digital wrongdoing action identification system.

LITERATURE REVIEW

Different clients get their records in the long-range informal communication site with iPhone, Android portable, Tablets, Desktop, lap or other electronic contraptions. The clients can skillfully refresh their profile data and furthermore, they can post any remark, transfer their photograph, waste their posting, content different clients, transfer music and video in their profile. They can make their profile all the more enthralling among their Facebook companions. With this site, correspondence medium is picked by the clients with the assistance of different computerized objects that is thusly associated with the companions the individuals who are staying far from them.

Web customers are allowed to use their records in the relational connection site for the most part or in helpful route keeping in mind the end goal to make their own profile presentation page on the page and there must never again be assigned any enlistment charge while a bit of the new customers need to make their profile or join with others in the Facebook social order. Young people use long-range relational correspondence site in broad whole. The diagram happens that bigger part young people contribute their vitality generally on the Facebook casual group. Well-ordered there is an addition to relational association site customers over the world. In India in 2015, about 2500 million customers were having their profile account on this site. The uttermost customer’s part covers youngsters in India. To complete Facebook Impact more as a drawing in Social Networking Site (SNS).

Chomp et al [3] composed on settling on how non-open data is executed on the web and online long range informal communication. He moreover perceived the peril plan that ends up the customer's insurance, in conclusion, recognizes a better strategy than propose high security keeping in mind the end goal to deflect prosperity breaks. The contemporary circumstance was spotlight for utilizing social gathering and moreover included the risks which impact the customers. Finally, they communicated some protection discernment that may be penetrated to be extra aware of relational association threats.

Gangopadhyay and Rishi have posted a record in which they have seen that Social locales attract energetic adults and permit them opportunities to existing together with regarded and darken individuals. Impacting amigos with cloud people and including them to their mates to list are in all probability thinking about as classy or as issues that can be asserted off. So they concentrated on how and to what degree the revealing of private information by strategies for customers is crazy. Besides, security settings made are based in sharp on the long-range relational correspondence goals like Facebook, Google Myspace, Orkut, Twitter and whatnot [4].

As per Information Technology Act, 2000 Cyber Crime is "most likely culpable by means of the method for the Information Technology Act". It isn't thorough in light of the fact that the Indian Penal Code, in addition, offers numerous cybercrimes, together with email mocking and digital maligning, sending, debilitating messages [5].

In Al-Jane K. B. S., they give a proposed structure for the terrible conduct and guilty party records examination and affirmation utilizing Decision Tree Algorithms for records class and Simple K Means set of systems for data gathering. The paper tends to help authorities in going over styles and changes, making measures, discovering affiliations and feasible reasons, mapping criminal systems and appreciating fitting suspects. This write-in light of particular gathering the terrible practices, according to the sort, place, and time and varying attributes; Clustering is constructed totally in light of finding the relationship among incredible Crime and Criminal trademark having a couple of once in the past cloud standard characteristics [6].

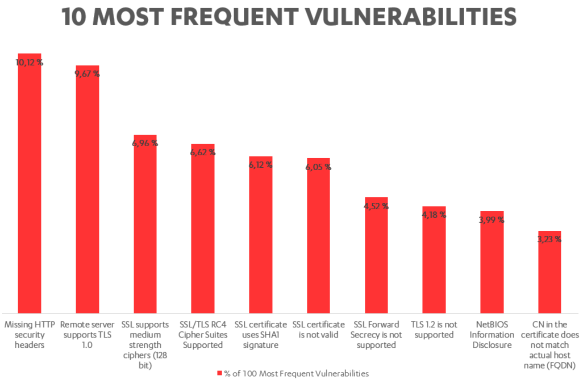
F. Stutzman and J. Kramer-Duffield give appeal on the most capable technique to update the security of customers on the individual to individual correspondence goals. To keep up a vital separation from recognizing confirmation of hacking, they incite making the F. Stutzman and J. Kramer-Duffield give the guide on the best way to deal with the upgrade the security of clients on the individual to singular correspondence areas. To abstain from perceiving check of hacking, they counsel making the client profiles, particular data for closest mates, on the off chance that you need to reduce the affirmations about security risks on Social Networking goals [7].

A. E Varma et al. proposed a decentralized and controlled structure that stick the security and certification of the customers in long-range social correspondence regions. The higher the security its protection will be higher by the utilization of a cryptographic approach like RSA and electronic stamp [8]

James et al. proposed the controlled structure that sticks the security and affirmation of the clients in long-range social correspondence territories. The higher the security its insurance will be higher by the use of a cryptographic approach like robotized technological development [9].

FRAMEWORK AND SCOPE OF THEPROPOSED WORK

Comprehensive the web is being gotten to by colossal people inside their restricted zones. Precisely when the customer and server trade messages among each other, there is an action that can be found in log records. Log files give a point by point depiction of the exercises that happen in a system that demonstrates the IP address, login and logout terms, the client's lead and whatnot. We have related the information tunneling procedures for seeing the Denial of Service assault. This sort of trap is to an incredible degree unsafe as it endangers the IT assets. It makes the server possessed by pantomime messages and reiterated questions. The server is congested by action packages, in order to reduce the server execution.



Frequent Vulnerabilities

A. Limitations of Existing Anomaly Detection/Prevention Systems

The impediment of information enrolling is the security issues of information figuring. It comes to comprehend that there are no wellbeing endeavors accessible for secure information figuring Users has genuine worries over assembled of delicate data. Security isn't suited basic information being set up in people when all is said in done open cloud. The current system is a gateway to attacks and hackers and needs to be more secure to be trusted by users. The flow of data is abundant and hence security is compromised which again gives way for attackers to misuse the system. The standard security issues join client information protection, information security, affirmation, information figuring affiliation and appropriated enrolling stage predictable quality. Clients ought to have the advantage of the supervision and have a study of scattered figuring associations for absolutely guarantee the security of client information. The information must be shielded from sullying, worms and Trojan in passed on preparing stage inside the course of action of inside and outside and this limitation has to be overcome by the data mining technique we have proposed which promises a secured network for communication.

B.Framework and Design Methodology:

Information mining can be elaborated as anexposure of sudden representations and new infers that are "hid" in wide databases. The utilization of data mining in this paper is to give the dealt with information from unstructured information of judge. In this paper the Data Mining methodologies for computerized bad behavior in two ways they are as indicated by the going with: --

i. Categorization of Cyber Crime
ii. Clustering Technique of Cyber Crime

1. Categorization and Classification of Cyber Crime:

DigitalCRIME is described as "an exhibition or the commission of a showing that is unlawful, or the oversight of a commitment that is told by an open law and that makes the liable party in danger to train by that law". Digital wrongdoing is insinuated as an entire thought that is described in both genuine and non-legitimate sense and which are under the Cyber Crime IPC ACT which includes the following:

i. Offenses by Servants(Public)
ii. Obliteration of Electronic Record
iii. Conning
iv. Impersonation
v. Data Theft
vi. Criminal Breach of deception, Debit Card
vii. Copying (Currency, Stamps, property)
viii. False or Fake Evidence IPC ACT.

2.ClusteringTechnique ofCyber Crime Clustering:

Information bunching is a strategy of putting relative data into gatherings. A bundling estimation sections an enlightening list into a couple of social occasions to such a degree, to the point that the equivalent is inside a get-together is greater than among get-togethers. Gathering can in like manner be seen as the most basic unsupervised learning framework; thusly, as each other issue of this kind, it oversees finding a structure in a collection of unlabeled data. There are such a critical number of procedures used as a piece of grouping, in this paper just K-meanscomputation algorithmis used.

C. Scope of the Work

The work proposed in this paper can be upgraded and developed for higher versions of security concerns and measures to enhance the security of the network, moreover, this implementation can be used for a wider network and a heavy traffic flow which will result is similar effective results and conclusions. This will enhance the risk management of the system and will make it more robust against attackers. This approach is implemented and used in many fields of data studying and analysis, data compression, computer study with specialization in biology which involves datasets and their study and can be used to develop a relationship between different datasets and enhance the ability to get structured data from a large set of un-structured data.

1. *ClassicOutlierApproach*:

Whatever special cases are found in a dataset in view of trades. Coincidentally, issues keep on existing to apply mining frameworks on data, for instance, emphasis of gigantic enlightening lists,and openness of uncertain information.

2. *SpatialOutlierApproach*:

The articulation "spatial" means or implies the articles that are accessible in space or have a land presence. Spatial Outlier suggests spatially implied dissent whose non spatial regards are likewise one of a kind in a comparative locale.

ARCHITECHTURE OF THE PROPOSED WORK:

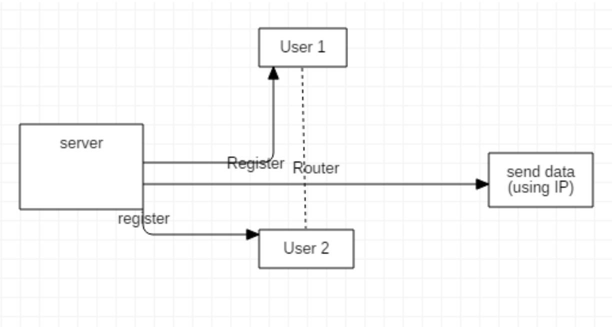


Figure 4.1 Architecture Diagram

The architecture revolves around the base station which acts as a server which will ensure a safe communication between the client and receiver and will enhance the security of transferring of the file and the algorithm is related to the unmistakable data mining methodology called as illustration affirmation on the log report. The client will be sending the files required by creating a request to the server which is the base station and once the base station verifies the user and checks the IP Address of the user, the sender can send the files they wish to and the verification of the files will be taken place by the Pattern recognition algorithm which will find malicious data and rectify Denial of Service Attack and hence by this approach we can see the refinement of affiliation strike easily as in DoS catch, the assailant or the item assemble sends same specific requests remembering the ultimate objective to calm the server execution.

- An extremely efficient data mining technique is applied on the log file with a predefined threshold value. The algorithm is named as pattern recognition and as the name signifies we detect malicious activities by mining the data and finding patterns within unstructured data to get a more accurate structured set of data.
- The algorithm works agreeing like when the server recognizes a numerous number of comparable solicitations that are being denied ceaselessly more than the preset limit esteem, at that point, we accept that an assault happens and the head is educated. By this approach we can recognize the dissent of administration assault effortlessly as in Denial of Service assault, the aggressor or the programmer sends same numerous solicitations with a specific end goal to moderate the server execution which will result in crashing of the server and disabling of the website to users which is a breach of security.

IMPLEMENTATION OF THE PROPOSED WORK:

In this research paper, we analyze about Cyber security, propelled encroachment their sorts, gathering, quirks and representation confirmation. We have related the unmistakable data mining methodology called as illustration affirmation on the log report. We set an edge respect. In the event that the measure of comparative asking for is gotten at the server, which is more basic than the most extreme respect, we expect this as a strike and the authority is been instructed. By this approach we can perceive the distinction of association assault effortlessly as in Denial of Service snare, the aggressor or the product build sends same particular demands keeping in mind the end goal to soothe the server execution

A. *Stages of Implementation:*

In our paper, we have shown the possibility of information mining systems to perceive digital assaults. Our point of convergence of thought would be on "finding designs" in a log archive (records that occur in the structure) which shows the progression of occasions and suspicious users and detection of attacks. From this log record, we perceive designs which fundamentally is the information having a comparative example. This is getting bunched information from an un-grouped informational index. In the first place, we use the grouping method to locate the sort of cybercrime, Denial of administration attacks. As we understand that grouping is the social occasion of data that has tantamount features. So this social affair discovers near cases of data that happen dependably in the logrecord.

Stage 1: Evaluate the user credentials:

The files are being communicated from the client or the customer to the receiver and the algorithm makes sure that the files and user are valid and unique which means no tampering with the user details and login credentials can take place. Information mining is brought in the scenario in the next step as the log files which have to be transferred and checked by the algorithm which verifies the uniqueness of the user and the data transferred.

Stage 2: Evaluate the Data

The data which is being transferred is mined under the algorithm proposed and once done, we get a set of structured data from unstructured data which is the reason we mine the data. This involves the data mining of the data present in files and check for duplications and ensures secured transfer.

Stage3: Traffic Analysis

Traffic Analysis refers to analyzing the traffic in the network which includes various clients sending and receiving files and this is extremely important as this step is the primary step of accessing the IP Address of the unauthenticated user who could be attacker or hacker. This traffic analysis includes the verification and deep mining of data which is done with the means of K means algorithm using JAVA Coding and this enables the entire traffic flow to undergo the analysis where the data is clustered and the clustering algorithm is bought to work. The data which is similar is clustered and is check for any malicious content as too much similar data means redundancy of data and this also can be a chance of multiple requests to the server at the same time which results in Denial of Service and can hinder the security and transfer of data in the system. The algorithm with have a data set and will keep it as a basic data set with which it will compare the progressing incoming data and resulting in this similar data are clustered together as a single data set and are checked for any malicious behavior which is done by IP Scanning which recognizes the IP Address of the suspicious user and blocks it. This Analysis also includes malware and other virus detection.

Stage 4: Scan the IP Address

This is the focal step of our algorithm as we have already mined and scanned the data in the previous step and hence we are able to locate the malicious data which basically refers to the attacker who is usually malicious data and techniques to hack the network and also gives way to Denial of Service attack as this malicious data and request from the attacker will hack the system and will cause the temporarily disabling of the website due to excessive load on the server.

This also refers to checking for attackers who are having unauthorized access to the system and are detected and blocked. Moreover, the attacker can use private data to get access to other user’s data and tamper the network security.

Once the malicious or suspicious data flow is recognized by the algorithm, the system will acquire the IP Address of the attacker which will be redirected to the user email Id and will be immediately blocked by the base station and hence the attacker will be blocked after the mining of data is done and any malicious activities are suspected. One great advantage is that after the attacker getting blocked from the base station, the user is also informed about the attacker and the IP Address used by him/her and the user can take security measures by blocking the attacker in any device they wish to enhance security.

Stage 5: Location Detection

Once the system has recognized the unauthorized IP Address, the algorithm uses the GPS Locations on maps to locate the location of the IP Address of the attacker which is re-directed to the user and police officials in case of emergency to track the attacker and do the needful and this is being implemented using JavaScript Code.

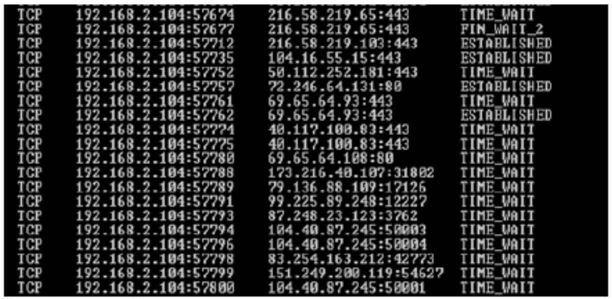
B. HardwareRequirements

Processor: Intel Core 2
Speed: 1.1 GHz
Hard Disk: 250 GB.
Monitor: SVGA
Mouse: Optical
Ram: 1GB

C. SoftwareRequirements

Working System : Windows95/98/2000/XP/7.
Application Server: Tomcat6.0/7. X.
Front End: Java, HTML, CSS
Scripts: JavaScript.
Server side Script: Java Server Pages.
IDE: Eclipse/Net beans
Back End: MYSQL 5.0/Heidi SQL 8.1
Database Connectivity: JDBC

Absolutely when the above strategy is actualized, we will record that data which contains standard portrayals what's more sporadic cases (malicious). By using the clumping strategy, we see the data that happen perpetually. Windows Server that keeps up the database. At first, we run the data that contains zero assaults and a while later add them to the ace archive or log record. The ICMP (Internet Control Message Protocol) will influence the framework to sit still by sending the voluminous measure of "ping" charge. Exactly when the above method is finished, we will record that data which contains run of the mill illustrations and besides strange cases (toxic). By using the gathering methodology, we recognize the data that occur on and on and perhaps malignant and use the Windows Server to keep up the database which is the base station which affirms the data which is sent and got and secures the affiliation made between the client and server as it will check if the affiliation is from the true blue customer and if the records or data traded are being traded under secured conditions and affiliations and moreover will check for vindictive ambush including hacking and DOS .Presently the information that contains the basic exercises and the information that contains strikes are encountered the system that we have proposed. In the event that the perspective of the log record indicates standard direct then they will be slighted.



```
TCP    192.168.2.104:57674    216.58.219.65:443       TIME_WAIT
TCP    192.168.2.104:57677    216.58.219.65:443       FIN_WAIT_2
TCP    192.168.2.104:57712    216.58.219.103:443      ESTABLISHED
TCP    192.168.2.104:57735    104.16.55.15:443        ESTABLISHED
TCP    192.168.2.104:57752    50.112.252.181:443      TIME_WAIT
TCP    192.168.2.104:57757    72.246.64.131:80        ESTABLISHED
TCP    192.168.2.104:57761    69.65.64.93:443         TIME_WAIT
TCP    192.168.2.104:57762    69.65.64.93:443         ESTABLISHED
TCP    192.168.2.104:57774    40.117.100.83:443       TIME_WAIT
TCP    192.168.2.104:57775    40.117.100.83:443       TIME_WAIT
TCP    192.168.2.104:57780    69.65.64.108:80         TIME_WAIT
TCP    192.168.2.104:57788    173.216.40.107:31802    TIME_WAIT
TCP    192.168.2.104:57789    79.136.88.109:17126     TIME_WAIT
TCP    192.168.2.104:57791    99.225.89.248:12227     TIME_WAIT
TCP    192.168.2.104:57793    87.248.23.123:3762      TIME_WAIT
TCP    192.168.2.104:57794    104.40.87.245:50003     TIME_WAIT
TCP    192.168.2.104:57796    104.40.87.245:50004     TIME_WAIT
TCP    192.168.2.104:57798    83.254.163.212:42773    TIME_WAIT
TCP    192.168.2.104:57799    151.249.200.119:54627   TIME_WAIT
TCP    192.168.2.104:57800    104.40.87.245:50001     TIME_WAIT
```

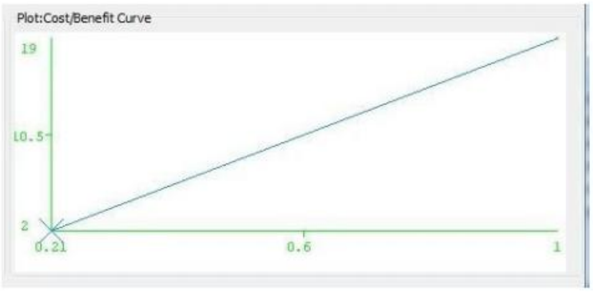
Figure 4.2 Sample Log File

EXPERIMENTAL RESULTS

Exactly when the customer and server exchange messages among each other, there is a development that can be found in log records. Log records give a bare essential depiction of the activities that occur in a system that shows the IP address, login and logout terms, the customer's direct et cetera. There are extensive assaults occurring on the web. Our purpose of the union of research in this paper is recognizable proof of Denial of Service (DoS) attacks with the assistance of case affirmation methodology in information mining and also in tracking the IP Address of the attacker and other malicious data is detected throughout the system and ensures security in the network. Through which the Denial of Service strike is seen. Foreswearing of association is a to an incredible degree perilous attack that jeopardizes the IT assets of a relationship by completed the process of stacking with emulate messages or unmistakable deals from unapproved clients. Consequently, switch at long last dissecting and enrolling an information spouting with IP address. The table shows the main result of the implementation of the user data described in table I. Figure 5 shows the graph of the cost-benefit analysis of the hard and soft classes. The graph obtained is a straight line, which signifies the accuracy of the implementation.

A. *Techniques Implemented:*

i. Validation of the Users
ii. Validation of Data and File Transfer
iii. Traffic Analysis
iv. IP Address Recognition of the Attacker
v. Location Detection
vi. Malware detection and removal
vii. Tackle Denial of Service Attack
viii. SQL Injection
ix. Hacker Detection



Cost Benefit curve

CONCLUSION

Modernized trap confirmation is imperative in the present web condition. The mix of substances, for instance, the wide difference in the web, the epic budgetary possible results opening up in electronic trade, and the nonappearance of significantly secure systems make it a fundamental field of research. A convincing on the web cybercrime improvement perceiving affirmation structure should have the capacity to discover both recommended and new ambushes as appropriate on time as could be run of the mill in light of the current situation. The certification methodology should act routinely adaptable to draw in the system to deal with the continually hinting at change nature of online strikes. The cream of the trademark and abuse an area models can overhaul cybercrime improvement revelation and securely permit sound trade. This algorithm utilizes an adaptable calculation for building clusters of data to recognize the cybercrime where the arranging data gathering changes ceaselessly and develops a few levels in just a single explore the arranging database, acknowledging top of the line get than the present methodology eventually. The accuracy of the proposed work is 95.67 % and it adequately observes the false rate quirks. This examination focused on client level anomaly and batter obvious confirmation. Later on, to achieve in a general sense secure trade we will widen this structure for scattered level cybercrime improvement zone in like route by profiling the framework lead.

ACKNOWLEDGMENT

This work was done on fulfillment of my final year project work with the guidance of P.Gayathri -Associate Professor, Department of Computer Science, VIT-University, and Vellore. Thanks to Gayathri mam for her valued guidance which was of optimum support to complete this Journal.

REFERENCES

[1] Cheww M., NayikderS.,How Journal of Scientific and Research Publications 5(1) (2015).

[2] Adnirora A., Shaikh H., Privacy in Online Social Networks (OSNs), International Journal of Advanced Research in Computer Science and Software Engineering 3(5) (2017).

[3] Ananthula S., Abuzaghleh O., Alla N.B., Chaganti S.B., Kaja P.C., Mogilineedi D., Detecting privacy in social networks, International Journal of Security.

[4] ManaA., Babloo S.San intelligent analysis of a city crime data using data mining, International conference information electronic engineering 6 (2012)

[5] Kumar A.M., Sharma B.N., Shrivastava S.K., Online Social Networks:Privacy Challenges and Proposed Security Framework for Facebook, International Journal of Soft Computing and Engineering 4(1) (2015)

[6] Hosseinkhani J., Ibrahim S., Chuprat S., Naniz J.H., Web Crime Mining by Means of Data Mining Techniques, Research Journal of Applied Sciences, Engineering & Technology 7(10) (2013), 2027-2032.

[7] Liu Y., Gummadi K.P., Krishnamurthy B., Mislove A., Analyzing facebook privacy settings: user expectations vs. reality, Proceedings of the ACM SIGCOMM conference on Internet measurement conference (2011), 61-70.

[8] Tollenaar N., van derHeijden P.G.M., Which method predicts recidivism a comparison of statistical, machine learning and data mining predictive models, Journal of the Royal Statistical Society: Series A (Statistics in Society) 176(2) (2013), 565–584.

[9] Conti M., Poovendran R., Secchiero M., Fakebook: Detecting fake profiles in on-line social networks, Proceedings of the International Conference on Advances in Social Networks Analysis and Mining (2012), 1071–1078.

[10] Zope A.R., Vidhate A., Harale N., Data Mining Approach in Security Information and Event Management, International Journal of Future Computer and Communication 2(2) (2013).

[11] P. Mell and T. Grance, “The NIST Definition of Cloud Computing Version 15,” Nat’l Inst. of Standards and Technology, Information Technology

[12] SeongMinYoo, Pyunnng Park, JiniSeop Shin, Jin oh, HoYongRya, JaeCheolRyou. “User-Centric Key Management Scheme for Personal Cloud Storage” ,2013 IEEE

[13] Wu Suyan, Li wenbo and Hu Xiangyi. “Study of Digital Signature with Encryption Based on Combined Symmetric Key”, 2009 IEEE.

[14] Deepti Chatterjee, NavdeepDasgupta and AsokeNath. “A new A-Symmetric Cryptography Algorithm using extended DSA method: IEEE 2012