International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-1, October, 2019

A Psychoanalysis of Data Privacy Maintenance Issues in Social Network using Data mining

P.S Arun Kaarthi, S.Sathiyabama

Abstract: ***The existing data sharing systems relates with the on-line social networks (OSNs) suggest encoding of information before sharing, the multiparty get to the executives of scrambled information has turned into a troublesome issue. A safe information sharing subject proposed in OSNs upheld figure content approach trait based and Elliptic Curve Cryptography algorithmic principle re-encryption and mystery sharing. The work relates the gatekeeper clients' delicate information grants clients to redo get to approaches of their information thus source scrambled information to the OSNs administration provider. The proposed technique displays a multiparty get to the executive's model that enables the communicator to refresh the entrance strategy of figure content. The characteristics fulfill the common access strategy. The work needs a fractional mystery composing development inside which the calculation overhead of client is essentially diminished by strengthening the vast majority of the mystery composing activities to the OSNs administration provider. Moreover, the check capacity on the outcomes originated from the OSNs administration provider to guarantee the rightness of fractional decoded figure content. The present subject partner affordable properties disavowal philosophy that accomplishes each forward and in reverse mystery. The insurance and execution examination results demonstrate that the arranged subject is secure and efficient in OSNs.***

Keywords: Social media monitoring, secure data retrieval, Key-Policy ABE and Elliptic Curve Cryptography Algorithm, photo privacy.

I. INTRODUCTION

A social network could be a structure created from actors like people or organizations, and ties between these actors like interactions, relationships, and connections. The literature for describes a graph to visit the social graph. The node of such a graph represents the association in tending performer and therefore the edges represent ties between those actors. A web social network is totally different from a social network. The two square measures normally used interchangeably. Apparently, a web social network would possibly comprise a whole social network concentrated act solely among the overall social network. In addition to that a social network could be a laptop software system and hardware system that tries to model the social networks found naturally within the world. A web social network contains a design of a user with a profile. The person's social links, though different services square measure usually incorporated.

Revised Manuscript Received on October 30, 2019.

* Correspondence Author

P.S Arun Kaarthi*, Guest Lecturer of Computer Science, Muthurangam Government Arts College, Vellore- 632002, Tamilnadu.

Dr.S.Sathiyabama, Assistant Professor of Computer Science, Thiruvalluvar Government Arts College, Rasipuram- 637401, Namakkal(DT), Periyar University, Tamilnadu

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

On-line social networks square measure sometimes internet primarily based and that they virtually ne'er utterly match the underlying social network they are making an attempt to model. Most on-line social networks nowadays follow the shopper server design that's common on the online. Though, distributed social networks square measure well studied within the literature. The term "online social network" (OSN) is employed to visit such a system of constituent and software system. The term "social network" (SN) is employed to indicate the begin shapely or approximately using the entire social network employees the social graph.

In any on-line social network, there is a wealth of data regarding its users embedded within the social graph. Specifically, there two sorts of data, specific and implicit. Specific data is data that's expressed by the user deliberately. The data contains the relation with the birthday that seems on a user's profile page. The specific data are not essentially correct. The implicit data are conjointly. The data can be inferred with a few users or a community supported specific data. The data can be recognized by a user is connected to several different users that have all expressed aims as fascinated by muscle cars on their profiles. The user can additionally fascinate by muscle cars. The implicit data is additionally not perpetually Implicit data is additionally not perpetually correct. In fact, it's higher finite in accuracy by the specific data on that it depends. Curiously, implicit data is sometimes quite near to this bound.

Much of the knowledge that's usually revealed by users in a web social network is especially sensitive. The sensitive information implicates and expresses the privacy and security issues are raised. All parties concerned face a contradiction in terms. The additional information is critical to form the OSN thrive. Users, however, maintain their privacy by not commercial enterprise personal information concerning themselves. The downside will be solved by protective user data and is mentioned extensively in the role. The work covers varied solutions for safeguarding user data from attackers at varied vantage points as well as users with direct access, indirect access, advertising agencies, and therefore the OSN suppliers themselves. All of those sections address protection of user data except for Associate in Nursing OSN to thrive the right operation of same social network should even be maintained. The text covers varied threats to the operation of OSNs were mentioned. At present the spreading of spam messages through Associate in Nursing OSN is extremely common. In addition, there's a notion of trust in a web social network between users. The trust verified using the content and the extended to stop the infective agent unfold of spam through the net social network. The several OSNs for the internet primarily based on general internet a pair with the security may be concern. The attackers may produce faux "sybil" accounts that they will utilize to influence the end result of elections in Associate in Nursing OSN.

II. HISTORY AND DEVELOPMENT OF SOCIAL NETWORKING

Offering information and human movement to people has been around for whatever length of time that people are near. anyway, once PCs and subsequently the net ended up unquestionably progressively normal, we tend to saw the use of email frameworks and short instant messages. The primary stage proposed that of correspondence between people [4]. This wasn't accordingly hazardous because of it concerned the causation of first message at once between two people exclusively, and it had been no more dangerous than causation elective information over the online to just a single individual. A great deal of advancements like visit rooms and on-line amusements became, thus web-based life wherever clients may share information, talk, examine interests and likes, post film and video, and so on one among the essential interpersonal interaction destinations like this was Myspace [2]. Its unique gathering of people was adolescents and subsequently the music and craftsmanship scene. A quality conceived on kind of a stone once Facebook went ahead line thus it turned into the chief in style informal organization. A few destinations, as LinkedIn or Flickr, have a specific reason, and a couple of territory units a great deal of general**.** There may be virtually no limit to what individuals will post on-line recently, and this can be a probably shuddery issue. The social media "spread quickly and wide and contain large-scale data of a broad audience. However, the unstructured large knowledge dealings might overwhelm users with data overflow" resulting in a variety of chaos. In the social media sites [2] and chat rooms area unit primarily simply "organizational and software system procedures the exchange of social data in social networking sites, text electronic messaging, instant traveler programs, bulletin boards, on-line role-playing games, computer-supported cooperative work (CSCW), and on-line education." As referenced in [4], locales that offer these sorts of administrations to clients at next to no to no value offer heaps of temptation for people and turned out to be very mainstream. The U.S.A an article was upscale history for online networking, has perpetually been a promising idea that John Drew a few clients, specific sorts. The usage of online life these days among teenagers is kind of all inclusive. The accomplishment of a social stage is fundamentally eager about its structure, which directs the character of the communications which will happen. The critical to see the discussions might be caught by others, it offers ascend to presumably unmistakably all the more intriguing association among clients. The modification embarking to turn out to be clear wherever the dangers region unit amid this, with the blend of person to person communication being actually simple to access by teenagers and people WHO don't appear to be security/protection mindful.

SPAM

Spam square measure undesirable or excluded messages sent to on-line email or online life account holders. Regularly, such messages square measure malignant, albeit some have needed to utilize it as cutting edge procedure. The use of spam goes back to once correspondence systems came into utilization on the net, and that they have full-developed with the advances inside the correspondence systems, to not upgrade it anyway as a dodge the very much expected correspondence of the legitimate record property holders. Overview have appeared inside the half of 2013, the development of social spam media has up to thirty fifth basically on average record, taking note of that one in everything about social posts contain spam (Nguyen2014). Extremely, social spam square measure been move abuse totally extraordinary medium. These grasp content based, picture or picture based for the most part and uniform asset locator based. The uniform asset locator based for the most part social spam regularly precludes the content, misuse exclusively the connection for the client to see in this manner wetting the readiness of the clueless injured individual. Picture based generally social spam comes as drawing in pictures or commercials with the proficiency of the informal community clients to click it. This ordinarily drives the client to elective on-line PCs that move Trojans into the pc. The content based for the most part social spam is circulated in light of phishing. The insurance live to be guzzled amid this case is to utilize available message separating functionalities that square measure been given by the SNS that the client have made record with. In addition, their outsider applications that see significant informal organization security risk like spam.

III. LITERATURRE REVIEW

The enthusiasm of social destinations has been expanded and heaps of investigation papers are printed. Various them referenced the wellbeing issues with long range informal communication locales, breaking down the protection and along these lines the dangers that cybercrimes the web interpersonal interaction sites. Chewe et al. [1] fixated on anyway close to home data is being stricken by net and internet based life and conjointly referenced anyway the protection become a hazard and the best approach to allot security attention to prevent security break. They featured the current situation on exploitation informal organization and dangers that may affect the clients. At last they communicated some security mindfulness that might be drilled to be a ton of checked out interpersonal organization dangers.

Gangopdhyay and Barnes [2] have printed a report amid which they need referenced that social destinations draw in young people and grant them chances to encourage alongside well-known and obscure people. Making companions with obscure people and adding them to their companion's rundown could be contemplated as exquisite or as things that might be flaunted. All together that they fixated on nonetheless and to what degree the noteworthy of private data by clients is secure. They conjointly focused the wellbeing setting made by the long-range interpersonal communication destinations like Facebook, MySpace Orkut, twitter and so on. The analysts Gupta et al. [3] have printed a report amid which they need referenced that gratitude to the expanding nature of informal communication locales, clients turned into an objective for aggressors. Person to person communication locales territory unit based generally no social relationship among people. The people share most assortment of their own and delicate data in their social locales. The private data and basic openness, aggressor is following clients to start with them to play out certain activities.

A few locales endeavored to dodge those abuses, anyway aggressor's territory unit still ready to conquer those safety efforts. They conjointly contain issues the problems} incorporates a study on totally unique protection and security issues in social locales. The issues finish up security hazard, character take, physical dangers, and hacking, phishing, spamming and malware assaults.

Verma et al., [4] demonstrated that long range informal communication clients wittingly and accidentally post bound assortments of individual and delicate information that may cause huge mischief, hurt them. The mutual news, photographs, recordings, individual data and every development of reality exercise with family and companion's region unit worry of client protection. They conjointly attempted mindful clients the age making breaks of their security and advise them the work of ongoing protection saving setting of labeling photographs on social destinations.

Deng et al., [5] portrayed and estimated shifted security perspectives crosswise over very surprising SNSs exploitation the possibility of bits of shared data. They furthermore uncovered that, similar to antiquated sites, outsider areas track client's exercises in Social Networking Sites with the diverse to broad suppositions.

THE BENEFITS OF SOCIAL NETWORKS

Organizations square measure grip long range informal communication to develop an inside culture of joint effort. This might be easy to look at anyway this free progression of information will support profitability and self-rule [6]. The specialists performing on an undertaking can have important, current, and altered information readily available, and that they will spigot into a prepared assembled bunch of cooperative individuals in the smallest degree dimensions of the association. The external surface of the association, informal communication will encourage a business reach and collaborate clients, improve the customer skill, and deal with its total picture. A few organizations nowadays watch destinations like Twitter and Facebook, for instance, to focus in on the gab concerning their item and administrations. The on-line total representatives will advance new item or, if a business' name is powerless, utilize online life to move the dialog inside the correct bearing. The organizations conjointly benefit of on-line customer voices to frame a less difficult crusade, undefeated brands influence customer encounters as partner basic a piece of an item battle and life cycle. Consider, for instance, the achievement of Apple. The apple clients have a decent enthusiastic attach to the total and track the corporate and its item on websites, Twitter channels, and Facebook. In spite of the fact that profound is that the associations with Apple retail locations in certain urban communities have as of now progressed toward becoming tourer attractions. Any individual will analyze them on Twitter.

FACEBOOK

The three foremost well-liked options of Facebook square measure the power to feature Friends, update your standing and run applications like games and quizzes [7]. A "Friend" is anyone on the Facebook network whom you permit to examine varied levels of non-public info, like job, birth date, photos, cluster membership, comments and list of alternative Friends. The even play on-line games and keep others updated on your standard of living. The friends can even see Friends of Friends, which means people need to make contact with the many friend.

IV. PROPOSED WORK

We elucidate a numerous ascendible and on-line social media spam detection system for social network security victimization Apriori data processing formula, the message is going to be encrypted victimization ABE coding formula and re-encrypted victimization Elliptic Curve Cryptography formula. The method generates public, non-public and secret keys for data security and every data get the various keys combined and safer than alternative secret Sharing algorithms, and additionally need a tendency to suggest the look, execution and analysis of Blowfish, a scheme calculated to reinforce on-line time alone.

Blowfish enables clients to change over photographs into encoded pictures, that the clients exchange to OSNs the look, execution and examination of blowfish, a framework intended to fortify on-line pic privacy [8]. Blowfish enables clients to change over photographs into encoded pictures that the clients exchange to OSNs. Clients straightforwardly oversee get to the board to those photographs by means of shared keys that square measure independent of OSNs or elective outsiders. OSNs apply standard picture changes (JPEG pressure) to all or any transferred pictures along these lines blowfish gives picture cryptography and coding system that is tolerant to those transformations [9]. Blowfish ensures that the beneficiary with the best possible certifications will totally recover the main picture from the renovated rendition of the transferred encoded picture though the OSN can't derive the primary picture [10].

ALGORITHMS:

Elliptic Curve Digital Signature Algorithm Signing

For language a message m by sender An, abuse A's private key d

1. Ascertain e = HASH (m), wherever HASH might be a cryptanalytic hash work, as SHA-1
2. Pick an irregular number k from [1,n − 1]
3. Ascertain r = x1 (mod n), where (x1, y1) = k * G. On the off chance that r = 0, move to stage a couple .
4. Ascertain s = k − 1(e + dr)(mod n). On the off chance that s = 0, move to stage a couple .
5. The mark is that the join (r, s)Elliptic Curve Digital Signature algorithmic rule Verification

For B to demonstrate A's signature, B should have A's public key letter

1. Verify that r and s square measure integers in [1,n − 1]. If not, the signature is invalid
2. Calculate e = HASH (m)
3. Calculate w = s −1 (mod n)
4. Calculate u1 = electronic warfare (mod n) & u2 = rw (mod n)
5. Calculate (x1, y1) = u1*G + u2*Q half-dozen. The signature is valid if x1 = r(mod n)

Apriori algorithmic rule

General method

Association rule generation is typically broken up into 2 separate steps:

1. First, minimum support is applied to search out all frequent item sets in an exceedingly data.
2. Second, these frequent item sets and therefore the minimum confidence constraint square measure wont to type rules.

Discovering all continuous thing sets in an exceedingly information is extreme since it includes looking all potential thing sets (thing mixes). The arrangement of potential thing sets is that the power set over I and has estimate 2n − one (barring the vacant set that is definitely not a sound thing set). despite the fact that the components of the power set develops exponentially inside the scope of things n in I, practical inquiry is plausible abuse the descending conclusion property of help (otherwise called enemy of monotonicity) that ensures that for an incessant thing set, every one of its subsets are visit And so for a rare thing set, all its supersets ought to try and be rare . Misusing this property, conservative calculations (e.g., Apriori and Eclat) will see all continuous thing sets.

Apriori Algorithm Pseudo code

The system for Apriori (T, minSupport) {/T is the database and minSupport is the base help

L1= {frequent items};

for (k= 2; Lk-1 !=∅; k++) {

Ck= competitors created from Lk-1

/that is artesian item Lk-1 x Lk-1 and disposing of any k-1 estimate thing set that isn't/visit for every exchange t in database do{

#increment the include of all applicants in Ck that are contained in t

Lk = hopefuls in Ck with minSupport

}//end for each

}//end for

ReturnU k, Lk-;

}

As is regular in affiliation rule mining, given a gathering of thing sets (for example, sets of retail exchanges, each posting individual things obtained), the algorithmic guideline endeavors to search out subsets that are normal to at least a base range C of the thing sets. Apriori utilizes a "base up" approach, wherever visit subsets are broadened one thing at any given moment (a stage alluded to as applicant age), and groups of competitors are tried against the data. The algorithmic guideline ends once no any lucky expansions are found.

Apriori utilizes expansiveness first inquiry and a tree structure to check applicant thing sets speedily. It produces competitor thing sets of length k from thing sets of length k − one. At that point it prunes the competitors that have partner degree uncommon sub design, which keeps with the descending conclusion lemma, the hopeful set contains all continuous k-length thing sets. From that point forward, it checks the managing information to see visit thing sets among the competitors. Apriori, whereas traditionally important, suffers from variety of inefficiencies or trade-offs, that have spawned alternative algorithms. Candidate generation generates giant numbers of subsets (the algorithmic rule tries to fill up the candidate set with as several as attainable before every scan). Bottom-up set exploration (essentially a breadth-first traversal of the set lattice) finds any largest set S solely finally two | S | − one of its correct subsets.

Photo privacy

The design, implementation and analysis of blowfish, a system designed to reinforce on-line image privacy. Blowfish permits users to convert photos into encrypted pictures, that the users transfer to OSNs. Users directly manage access management to those photos via shared keys that area unit freelance of OSNs or different third parties. OSNs apply normal image transformations (JPEG compression) to any or all uploaded pictures therefore blowfish provides a picture cryptography and secret writing mechanism that's tolerant to those transformations. Blowfish guarantees that the recipient with the proper credentials will fully retrieve the initial image from the remodeled version of the uploaded encrypted image whereas the OSN cannot infer the initial image.

Blowfish

Blowfish was planned in 1993 by Bruce Scheier as a snappy, diverse to existing coding calculations such AES, DES and three DES and so forth.

Blowfish might be a symmetrical square coding algorithmic program structured in thought with,

- Fast: It scrambles information on monster 32-bit microchips at a rate of twenty-six clock cycles for each PC memory unit.
- Compact: It will keep running in yet 5K of memory.
- Simple: It utilizes expansion, XOR, seek table with 32-bit operands.
- Secure: The key length is variable; it is inside the scope of 32~448 bits: default 128 bits key length.

It is suitable for applications wherever the key doesn't change normally, similar to correspondence connection or partner degree programmed document encryptor.

Depiction of Algorithm:

Blowfish customary square figure algorithmic principle encodes square learning of 64-bits at once, which pursues the feistel arrange.

Key-extension:

It will change over a key of at the most 448 bits into many sub key clusters totaling 4168 bytes. Blowfish utilizes measure, which differs in measure of sub keys. These keys region unit producing prior to any encoding or decipherment. The p-exhibit comprises of eighteen, 32-bit sub keys:

P1,P2,… … .,P18

Four 32-bit S-Boxes comprises of 256 sections each:

S1,0, S1,1,… … . S1,255

S2,0, S2,1,… … .. S2,255

S3,0, S3,1,… … .. S3,255

S4,0, S4,1,.....S4,255

ABE ENCRYPTION SCHEME

1. Worldwide Setup: This algorithmic program takes as info a security parameter l and yields the framework parameters.

2. Specialist Setup (SKi, PKi, Ai). Each expert Ai produces his mystery open key attempt weight unit (1l) (SKi; PKi) partner degreed an entrance structure Ai, for i=1,2; . . .N.

3. Keygen (Ski,GID,Ai GID)Skui each specialist Ai takes as info his mystery key SKi, an overall image GID and an accumulation of characteristics Ai GID, and yields the key keys SKiU, wherever AiGID = AGID ∩Ai ,AGID and Ai indicate the properties taking after the GID and checked by Ai, severally.

4. Mystery composing (params, M, Ac). This algorithmic program takes as information the framework parameters params, a message M and a gathering of traits AC, and yields the figure content CT, wherever Ac= ˜Aci ∩ Ai.

5. Unscrambling: This algorithmic program takes as info a GID the key keys figure content CT and yields the message M, wherever Ic is that the list set of the specialists Ai such Aic≠

V. RESULT AND DISCUSSION

As way in light of the fact that the path forward for enormous data minds it's clearly that data volumes can in any case develop and, in this manner, the prime purpose behind that may be the commanding addition inside the assortment of handheld gadgets and web associated gadgets, that associateticipated} to develop in an exponential request. SQL can remain in light of the fact that the typical for data examination and Spark, that is rising, can rise in light of the fact that the complimentary apparatus for data investigation. Apparatuses for Associate in Nursing lysis while not the nearness of an examiner square measure set to require over, with Microsoft and Salesforce each as of late saying alternatives material belonging non-coders to shape applications for survey business data. According to IDC 1/2 all business investigation code can encapsulate insight any place it's required by 2020. In elective words it might be previously mentioned that prescriptive examination are built into business code. Projects like Kafka and Spark can alter clients to make decisions progressively. AI can have a way bigger task to carry out for data planning and prognostic investigation in organizations inside the returning days. Protection and security difficulties related with monstrous data can develop and by 2018, five hundredth of business morals infringement are related with data. Boss data Officer are a standard sight in enterprises inside the ongoing future tho' it's idea that it won't keep going long. Self-sufficient specialists and things like robots, independent vehicles, virtual individual right hand and reasonable gadgets are an enormous pattern inside what's to come. enormous data ability smash as is seen as of late can reduce inside the returning days. The International Institute for Analytics predicts that partnerships can utilize enlisting and inward instructing to growing data researchers to actuate their very own issues done. Organizations can presently have the option to buy calculations rather than program them without anyone else and add their very own data to that. Existing administrations like Algorithmia, DataXu, and Kaggle can develop during a gigantic scale, that is algorithmic program markets can rise. a ton of organizations can attempt to get their income from their data. The hole among knowledge and activity in enormous data goes to downsize and a great deal of vitality are given to getting bits of knowledge and execution as opposed to gathering gigantic data. fast and uncalled for data can supplant huge data. partnerships square measure expected to raise the right inquiries and make higher utilization of the data they need, a great deal of the huge data they need square measure unused as of late

VI. CONCLUSION

A sole resolution to social network privacy and security problems is to own some data of the ways that during which one will get fooled, do not post something not verified wish to cover from a interloper. The care takes for the WHO adds a "friend" since there is merely no means of validating a user's actual identity on-line. The proposed work projected a design for secure communication between the users and a secure request-response design for exchange of data between the users. The system needs the process of cleaning and updating. The senses to open whereas exploitation of the overall and not jump to conclusions. The analyses based on the content totally before doing something. There were not any free lunches during this world. So the web is not any completely different.

REFERENCES

1. Chewae M., Hayikader S., Hasan M H. and Ibrahim J. 2015 How Much Privacy We Still Have on Social Network?. International Journal of Scientific and Research Publications, Volume 5, Issue 1, January 2015 Edition,page no:1.
2. Barnes, S. (2006). A privacy paradox: Social networking in the United States. First Monday, 11(9). doi:10.5210/fm.v11i9.1394
3. Kumar, A., Gupta, S. K., Rai, A. K., &Sinha, S. (2013). Social Networking Sites and Their Security Issues. International Journal of Scientific and Research Publications, 3(4), 3.
4. Verma, A., Kshirsagar, D., & Khan, S. (2013). Privacy and Security: Online Social Networking. International Journal of Advanced Computer Research, 3(8), 310-315.
5. Deng, X., Bispo, C. B., &Zeng, Y. (2014). A Reference Model for Privacy Protection in Social Networking Service. Journal Of Integrated Design & Process Science, 18(2), 23-44. doi:10.3233/jid-2014-0007
6. Bertot, J. C., Jaeger, P. T., & Hansen, D. (2012). The impact of polices on government social media usage: Issues, challenges, and recommendations. Government Data Quarterly, 29(1), 30-40.
7. Gangopadhyay S and Dhar M. D. social networking sites and privacy issues concerning youths. Article – 2 Global Media Journal-Indian Edition Sponsored by the University of Calcutta/www.caluniv.ac.in ISSN 2249 – 5835 Summer Issue/June 2014/Vol. 5/No. 1.
8. Gunatilaka D. A Survey Of Privacy And Security IssuesInSocialNetwork.http://www.cse.wustl.edu/~jain/c se571-11/ftp/social/index.html.
9. Pesce and Casas Privacy Attacks in Social Media Using Photo Tagging Networks: A Case Study with Facebook [10] D. Boyd and E. Hargittai. 2010. Facebook privacy settings:Who cares?" Journal on the Internet, 15(8), 2010.
10. Krishnamurthy B. 2010. I know what you will do next summer. Acmsigcomm Computer Communication Review, 40(5):65-70, Oct. 2010.

AUTHORS PROFILE

P.S.Arun Kaarthi obtained his MCA Degree in Computer Application from VIT University, Vellore in 2009. He had Qualified SET in Computer science from Mother Teresa University, in 2017. He had Qualified UGC-NET in Computer Science from National Testing Agency, in 2019. Now he is working as a Guest Lecturer in Department of Computer Science at Muthurangam Govt Arts College, Vellore.

Dr.S.SATHIYABAMA obtained her M.Sc Degree in Computer Science from Avinashilingam Deemed University, Coimbatore in 1997. She had her M.Phil. Degree in Computer science from Bharathiyar University, Coimbatore in 2002. She received her Ph.D. Degree in the area of Data Mining in 2007 from Periyar University, Salem. Now she is working as an Assistant Professor of Computer Science at Thiruvalluvar Government Arts College, Rasipuram.