Applying Neural Networks to Cryptography

S. Muthamil Selvan M.S, S.Narasimhaiah, Y Sai Manikanta Reddy, B. Hemanth Kumar

Abstract: This paper is small part that investigates about methods involved in encryption of data by using cryptographic methods for cell phones and smart devices, by utilizing neural systems method.This is considered as the major problem because of increased in usage of mobile and tablets in mobile transactions across the world in place of conventional pc. The major goal is to provide strong authentication systems that can efficiently handle the encryption systems like: Strong Authentication (HTTS), Authentication system for mobile, Near Field Communication, advanced encryption system , one time password infusion withneural networks (in view of natural building blocks of neural network in human brain and how data stored, analyzed and retrieved)will provide strong authentication for the mobile phone users and I t also increases the mobile security standards. The main theme is to determine the foremost fusion of cryptography techniques in combination withneural network algorithms it provides formidable increase security over the authentication of the cell phones.This can be attained by inspecting and evoluvating of the cryptographic methods with neural network algorithms, using the NS-3 Network Simulator, Python SciPy Library under BSD. The outcomes and finishes of the examinations may fill in as a guide cell phones.

Keywords: Data Sets, Mobile Transaction.

I. INTRODUCTION

This paper is a thoughtof using the mix of strategies information science techniques to decide the most ideal approach to scramble synchronization of information between a PC and a cell phone.PC inside a private system, all in all, are more secure than portable PC. The Computer inside a venture are normally utilizing LAN not WAN system that is all in all increasingly secure what's more, Enterprise systems utilize numerous other security structures like for example Intrusion Detection Systems that are all things considered more secure than convenient firewall and they additionally give high security the serious issue is cell phones which are overwhelmingly more around the world when they are contrasted with ordinary gadgets.in recent year mobile device usage is more predominant than the pc,previously(before 10 years) many people had one or more computers and a mobile phone,homepc,etc.when it comes to present scenario everyone are using 1 or more mobile devices which runs on platforms like android,Ios, Microsoft Os,etc. when it comes past years where only Ios and Microsoft ,where android does not exist,so older versions are immune to malwares,virus ,etc attacks.since they were unfit to send get information or associate with the web, 2G telephones were just prepared to send SMS mms messages and make phone calls, around 2007 - 2009 everything changes with iOS and Android,Windows later on, But when itcomes to present scenario the mobile platforms arevulnerable to malware,virus,worms,etc...and also increased in hacking of mobile phones .so we need a strong authentication system which provide high security towards all the attackswhich in capable of handling the data of the device only understands by itself.Today in the event that you contrast android telephones and increasingly, at that point 6 screens or googles android , ios , windows they are great match and furthermore contender to numerous PC and workstations, with 3-12GB RAM, 4-56 cores for every Central Processing units s and 20 plus additional cores per GPU, as indicated by Gartner's most recent research numerous individuals not willing to utilize their PCs any longer on the off chance that they can do every last bit of it from their cell phones. These days the shopper advertise additionally shoves the applications for cell phones more than sites, there's most certainly not a mainstream brand like Kfc, Pizza hut, Croma , H&M that does not have an application for iOS ,Windows and Android. Since numerous individuals utilize their cell phones as essential information and communications technology devices holds numerous critical data working with it considerably more than on their normal PC (work area/workstation). portable installments frameworks created by Microsoft, Amazon, Google and Apples and numerous banks and numerous Cryptocurrency day to day is use by means of the cell phones, make the cell phones considerably to a greater extent an objective for programmers. Indeed, even with the best answers for security we hear regularly of a programmer that stole around 1000 million client accounts from Yahoo or of some data breach with its security weakness that influences the equipment segments with current antivirus orAuthentication System can prevent the programmers from taking personal information, as for instance the most recent Meltdown and Specter. we are recommending an answer in this paper proposes a strategical thought that when a programmer conceivably can take our information and unscramble by some brute force algorithms but when it turns that he don’t understand after decrypting the data which he received from hacked mobile or pc.Because we wrote them in a language that only our computer only understands it and this makes a new language that only our system only understands that language and interpret the data.what if we can implement this system to mobile phones and our computers (both ensured with irissecurity,

Manuscript received on 10 December 2020 | Revised Manuscript received on 12 December 2020 | Manuscript Accepted on 15 December 2020 | Manuscript published on 30 December 2020.

* Correspondence Author

S. Muthamil Selvan*, M.S, Department of Computer Science, SRM Institute of Science and Technology, Chennai (Tamil Nadu), India.

S.Narasimhaiah, Department of Computer Science, SRM Institute of Science and Technology, Chennai (Tamil Nadu), India.

Y Sai Manikanta Reddy, Department of Computer Science, SRM Institute of Science and Technology, Chennai (Tamil Nadu), India.

B Hemanth Kumar, Department of Computer Science, SRM Institute of Science and Technology, Chennai (Tamil Nadu), India.

with strong Authentication and Anomaly Intrusion Detection System that can distinguish in the event that it is you or not me by composing and what applications you use and when).

II. CRYPTOCURRENCY AND ENCRYPTION

So as to clear up how cryptographic cash like Bitcoins Ethereum, work we need to at first start talking about what is a blockchain and smart contracts.[1]

A. Block chain

Today blockchains are amazingly prominent, the most limited meaning it defines blockchain will be, blockchain is ainterlinkage of the blocks that contain a piece of information or data or significance. The procedure was initially clarified in 1991 and it was initially expected to be utilized for timestamping advanced records so as to anticipate predating or altering the first report. The block chain undoubtedly is a great technology so far invented by human the inventor of blockchain is SATOSHI NAKAMOTO in 2018 to give a service to bitcoin.

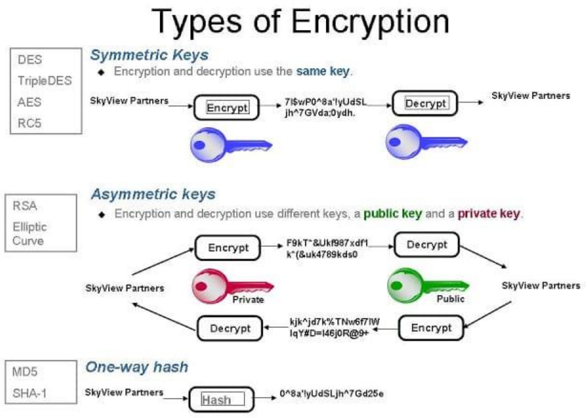
What is Blockchain?

It is a technology which allows a distributed digital information which cannot be copied generally it simplifies and enhances its protection of data.Originally devised for the digital currency, Bitcoin, (Buy Bitcoin) the tech community is now finding other possible uses for the technology. The Creator of the well-known cryptographic money Bitcoin utilize the blockchain strategy to make a disseminated record that is available to all clients of the system, so as to forestall altering. Every block in block chain holds a piece of information, the hash value of the previous block, and the hash estimation of its present block and previous block. The Bitcoin blockchain holds or stores information that has subtleties of an exchange, source beneficiary it is a measure of bitcoins inside that exchange. When a block is made the hash is determined and has interesting worth. The unique value resembles a unique mark, it checks the legitimacy about the information in the blockchain, since all blockchains it owns a unique set of esteem and the estimation of the past block, so when an approaching block (X) contains estimation of past block (Y) not the same as the estimation of the hash esteem that is put away inside the block (An), it implies with the block X has been messed with or it contains a mistake when it processed forward or sent, so on the off chance that you need to alter a block you have to change all blocks in the blockchain, and this process is exceptionally difficult because of the verification of-work, bitcoin processing time is around 10 minutes ascertain a block inside the blockchain. Likewise total block chain use something many refer to as a shared system where everybody inside the blockchain can unite, every friend audits the got block inside the blockchain, the process create it troublesome or practically unthinkable for somebody to alter the blockchain, it causes huge mess that just they need to alter and solve all hashes fortotalblocks yet they need to likewise mess with 60% plus of the companions inside a systems, that can be in 10.000 - 100.000 or even greater 1.000.000 given the prevalence of Bitcoin present day.[2]

B. Smart contract

A SC is a code running top of a blockchain helps you exchange money or another transparent values. like a crypto box that contains value and only unlocks if certain conditions are met,And SC eliminates the need for trusted parties. These transactions are trackable and irreversible. they are much the same as customary paper contracts yet just contrast is they are100% computerized from content, substance to a sigh, smart contracts in the digital money Ethereum. In astraightforward terms, Smart Contracts are traded for third gathering like razor pay and PayPal that need to deal with thecash and administrations you purchase from third party organization. If the client and specialist co-op provide confide in kick-starter to deal with their cash. Brilliant Contracts wipes out the requirement for an outsider when when it meet its terms or objective is achieve implanted in the Smart Contract cash is discharged to the specialist organization (when the specialist co-op begin the administration provided to client the smart contracts affirms provides cash to the specialist organization). smart Contracts utilizes blockchains are comparabilly provide more security over one server of a supplier of a cash administration like third party gathering administration kick-starter the safety provided by blockchain s clarified in the previous part. smart Contracts are the particularly centerpiece of it and utilized inside the digital currency Ethereum, the cryptographic money utilizes their own languages of programming called Solidity (like JavaScript), Bitcoins likewise bolster keen contracts however in a progressively restricted manner then Ethereum provided. [3]

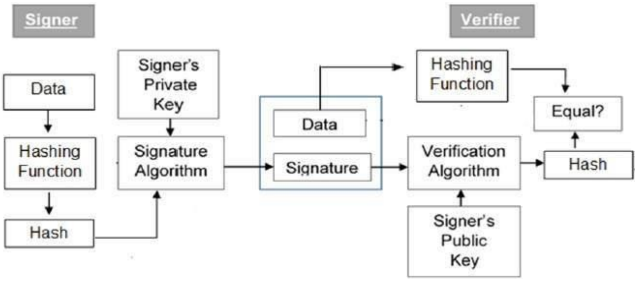
C. Encryption



The process of making regular message into a scrambled text that can be done with a phrase key to scramble the text from the regular message to encode into a scrambled text is called Encryption. Symmetric encryption is done to encode a text in to scrambled text with a phrase key and also it can be decoded by with same phrase key. It's unsafe in light of the fact that need to provide the passphrase likewise and if a third party gathering captures the text and phrase key peruse the message and like they are the recipient. To anticipate this uneven encryption was imagined, that implies that everybody has an open and private key. Source An and destination Z. in the event that Sender A needs to make an impression on collector B, the Sender encodes the message utilizing the public key of Receiver Z, with the goal that just beneficiary Z can decrypt the text utilizing it is very own private key.

Advance encryption system and PGP are increasingly well-known encryption convention. For instance, Bitcoin utilizes topsy-turvy encryption so as to make guaranty just a proprietor of a wallet can get the bitcoin.[4] [5]

III. SYSTEM ARCHITECTURE



This paper explains about how modern authentication process works and where we can apply our concept in this process. It appears in almost all security applications. Actually it's a mathematical function that converts a numerical data into some other numerical input data which compressed during the process. there are few popular hash functions like MD, SHA, ripemd, whirlpool for this hash functions are in range of 128 – 512 bit.Commonly used cryptographic hash functions includes MD% andSHA-1,wew although there are some other more hash functions are exists.
Hash function usesMessage Integrity Check ,send hash of message ,MIC always encrypted, message optionally ,Message Authentication Code ,send keyed hash of message ,MAC, message optionally encrypted,Digital Signature ,Encrypt hash with private key ,Verify with public key.
There are some other hash functions to create a one way password file to rainbow tablets and for intrusion and virus detection were to keep and check hash files on system like for examole tripwire.

IV. NEURAL NETWORKS, GENETIC ALGORITHMS

Neural Networks explained in a way assort structure or a black box,which draws numerous information sources. Which provides various yields of that input. For an instance as info, we provided a self-automated or self-driving vehicle (impediment inside 200m) it yields, we obtain one or more yields like control guidelines (take u turn in 500m) for oneself driving vehicle. Neural Network comprises of different little units or neurons, they are assembled into numerous layers. Neurons from one layer infuse of the other layer neurons of the following layer through calculations, gauged associations simply modify associations with an esteemed number joined to each other. neuron draws the estimation of an associated neuron and increases along with association weight the aggregate everyneuron associated with it.

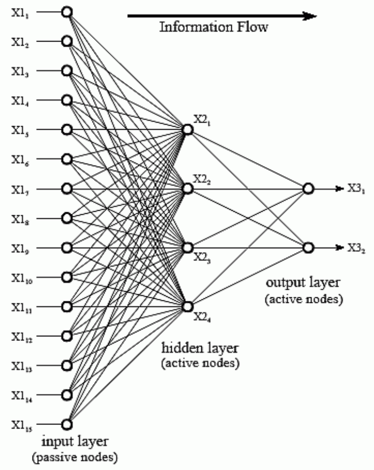
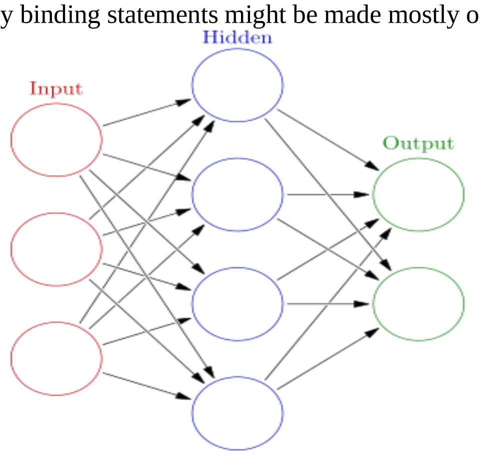


FIGURE 26-5
Neural network architecture. This is the most common structure for neural networks: three layers with full interconnection. The input layer nodes are passive, doing nothing but relaying the values from their single input to their multiple outputs. In comparison, the nodes of the hidden and output layers are active, modifying the signals in accordance with Fig. 26-6. The action of this neural network is determined by the weights applied in the hidden and output nodes.

The inclination of neurons in esteem then they are allotted to initiation work changes the esteem scientifically before it tends to be pushed into the following neuron. With provided data sources can proliferated inside an entire Neural network Proponents of keen contracts guarantee that numerous sorts of legally binding statements might be made mostly or completely self-executing, self-implementing, or both. Different digital forms of money have actualized sorts of keen contracts. They are additionally different kinds of nonpartisan systems like CNN or DNN. The widely utilized meaningabout a CNN is said to be a neural network they can share a parametersbetween two spaces, we provide a short information to provide a better understanding to it. We have a picture it's a three dimensional item with height and stature, the picture likewise has profundity for this situation, those are the RGB esteems for the picture. In the event that we take little piece of that picture apply neural networks on itto produces esteems H, on the off chance that we slide vertical way the little piece of picture over the unfilled space saved for the whole picture in the following process we don't change the values of weight. This will imply that we will get another new picture, with various tallness and various weight and in particular the profundity will be altogether different or the RGB esteems. Is said to be convolution and it defined by which tangled systems are framed with new factors about new part H, K, and so forth by remove a portion of existing neural network and shaping latest one.



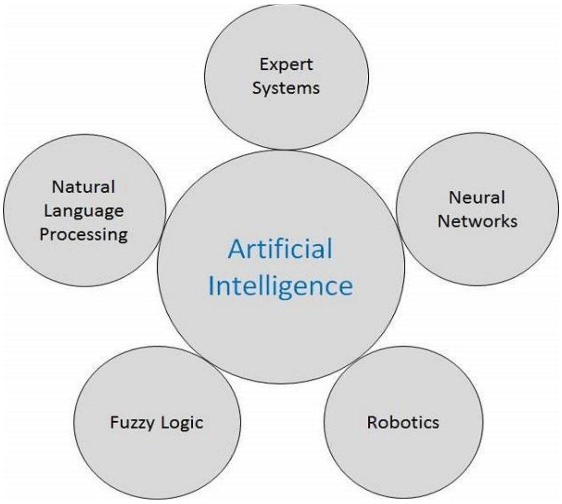
We should now discuss deep neural networks. Profound neural networks can hoard information in for some circles inside the .neural networks with latest information. We can provide a guide to clarify for better understanding. Least difficult clarification for deep neural networks is that deep neural networks is framed from numerous convolutional neural networks or convnet is going to essentially said a profound system where as opposed to having heaps of grid duplicate layers, we will have piles of convolutions. in the event that we clarify it with the past precedent the deep neural networks will be molded like a pyramid. The base layer will have the first picture huge and shallow with all R G B esteems, by utilizing the task know as convolution to shape convolutional neural networks we will crush the spatial measurements while expanding the profundity, the span of the pyramid relies upon the issue scope, and the classifier can be at the top. we have graphical portrayal of a deep neural networks shaped from different convolutional neural networks arrangement in this paper will utilize NN we belive that the neural networks are the major part of this paper for a best comprehension the peruser we use is(CNN).[6 - 8]

A. Genetic Algorithms

Today PC specialists and information researchers have huge information or expansive sizes of data to exercise, extensive datasets imply they can provide increasingly exact data from that enormous information, yet preparing huge volumes on information is an issue without anyone else. To respond to specific inquiries the old school approach is to proceed to look at every one of the information for the pertinent data. The latest methodology is called evolutionary algorithms calculate like the Genetic algorithms provide well-ordered guidelines for the PC to take care of the issue. These calculations are utilized today in numerous fields to take care of issues like plane eco-friendliness (for instance the best blend advancement of fuel weight and wing plane to progress further fuel utilization for predefined separate). Evolutionary algorithmsdependson biological or natural advancement, by and large and they are quickest method towards concocted about decent arrangement no reason to check each and every probability. Example, on the off chance that we can to produce another sort of different species that have ability to work quickest, along these lines, termed introductory populace stands arbitrarily created utilizing evolutionary algorithms, every new specieshavetheir own kind of attributes. we gather all species to test and analysis, for an instance to stroll for a specific timeframe, the two species that increased more separation contrasted, gathering can be done by other two different methods which are faster, since the dual quickest guardians we make another species with components since the two guardians alsominor transformation procedure that transforms some portion of the qualities related to new species. at that point, testing over and over for each new age, so after numerous ages, we locate the ideal answer for the issue without the need to experience each and every blend for each conceivable species. The most well-known Evolution Algorithms are said to be Genetic algorithms. [9] [10]

V. ARTIFICIAL INTELLIGENCE

AI is a way of making a computer controlled robot, or a software think intelligently.it is also known as machine Intelligence.it analize how human brain thinks, learn and to take care of the issue and afterward utilizing the result of this investigation as a premise of creating keen programming and framework applications like gaming, natural language processing, expert system, vision system, speech recognition, handwriting recognition and intelligent robots. In a point of view Artificial technology is a science and technology based on disciplines of all kinds of knowledges like such as computer science, biology, psychology, linguistics, mathematics, and engineering. Generally AI main goals to create an expert system (which behaves like human brain),and to implement high intelligence of human (taking own decisions etc.)



VI. EXPERIMENTAL ANALYSIS

Issue attempting to unravel: safely putting away the reserved and open computerized wallet label on a PC matches withwith other cell phone for wellbeing, likewise safely putting away the twelve reinforcement terms for an advanced wallet may be perused just with the help of mobile,PC of the proprietor. The answer: natural or biological calculation utilized nearby hereditary calculation in software engineering for more grounded encryption, utilizing artificial intelligence Deepneural networks, main aim to the accomplishment of the calculation hoard the wallet reinforcement key in NN. Generally, twelve words are encrypted utilizing new dialect. The new dialect how about we call it lantian is shaped utilizing chart as a neural system, it is framed utilizing hereditary calculation and utilizing your most loved picture where key begin witha to z. utilizing GA we get new ages, the development calculation do we include deduct to isolate or increase the two qualities in the quality to get one new esteem relies upon the dark scale benefit of comparing the pixel of the photo range from 0.0 black to 1.0 white for the first child gene If its 0-0,25 you add, if its 0.25 – 0.5 you subtract, 0.5 to 0.75 you divide, 0.75 to 1.0 you multiply, for the second child gene it goes 0-0.25 multiply, 0.25-0.5 divided. 0.5 – 0.75 subtract. 0.75 – 1.0 add.. Testing if the calculation for new dialect Lantian creation is OK we can test it all alone own pre translate words, so we can check how precise the algorithm resembles testing DARPA dataset for intrusion detection system.

Which provide words from another dialect as one piece of the riddle, and mathematical calculations provide another piece of the riddle, yet lacking of the key or photograph it is difficult to reproduce a similar language. Is a simpler process which recollect one photograph or what is your most loved photograph at that point to recall twelve words and record them on a bit of paper or content analysis on a personal computer. The mathematical calculations about the language which formed newly is said to be called asLantian in reserved in a deep neural networks for quicker preparing of new words and making an interpretation of them from and to Lantian. At that point the words encoded in the new dialect are traded utilizing topsy-turvy encryption between proprietors mobile and PC, for encryption key we utilize the KDD CUP 99 dataset because of its extensive volume of information. Key To the arrangement: make claim language utilizing precedent above, and reserve the twelve words in new dialect (just discernible to proprietors PC and cell phone),

read the information put away in a 3D created picture arrangement was made utilizing BSD. [16] [17] [18]

VII. CONCLUSION

This provides a conclusion that the system can be utilized to analyze and store the information from complex form to simple form, it can be achieved by current generation CPU and GPU but which cant store lot of data in a deep neural network, by applying ai to this method improves in pure evolution and enhancement of security where genetic algorithms withcrypto graph improves it to a unique level by applying ai to it improves alothere we are using a supervised technique to implement the technique where it helps analyzing the data and improves in greater extent.

REFERENCE

1. Andreas M. Antonopoulos, “Digital Cryptocurrencies”, 2014
2. Steve Tale, "Blockchain Technology: Story of Blockchain". 2017
3. Jeff Reed, "Smart Contracts: The Essential Guide to Using Blockchain Smart Contracts for Cryptocurrency Exchange", 2016
4. Margaret Cozzens, Steven J. Miller, "The Mathematics of Encryption: An Elementary Introduction", 2008
5. M. J. Raney, "Encryption", 2012
6. Raul Rojas "Neural Networks: A Systematic Introduction". 2013
7. Yann LeCun, YoshuaBengio& Geoffrey Hinton, "Deep Learning" Nature 521, 436–444, 2015, http://www.bioinfo.org.cn/~casp/temp/DeepLearning.pdf
8. Jurgen Schmidhuber, "Deep learning in neural networks: An overview. Neural Networks", 2014 https://arxiv.org/pdf/1404.7828.f
9. Dipankar Dasgupta, Zbigniew Michalewicz, "Evolutionary Algorithms in Engineering Applications", 2013
10. Omid E. David, H. Jaap van den Herik, Moshe Koppel, and Nathan S. Netanyahu, "Genetic Algorithms for Evolving Computer Chess Programs" 2014
11. MIT Lincoln Laboratory
12. http://www.ll.mit.edu/about/about/about.html,
13. Defense Advanced Research Projects Agency, http://www.darpa.mil/
14. 1998/1999 DARPA Intrusion Detection Evaluation Data Set, http://www.ll.mit.edu/mission/communications/ist/corpora/ideval/data/1999data.html
15. KDD CUP 99 Data Set, http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html
16. S. Gelev, A. Sokolovski, “Using GPU for query of email spam detection systems and IDS”, IT’14 ,http://www.it.ac.me/zbornici/ZbornikIT14.pdf
17. BSD, https://www.freebsd.org/
18. R, The R Project for Statistical Computing, https://www.rproject.org/
19. Octave Scientific Programming Language, https://www.gnu.org/software/octave/
20. github project code, https://github.com/lexqbit/lantia