Jan - Jul 2018

TRINITY INSTITUTE OF PROFESSIONAL STUDIES

Dwarka, Sector-9, New Delhi

Trinity Tech Review

Vol 4, Issue 1

Disclaimer: The views and opinions presented in the articles, case studies, research work and other contributions published in Trinity Tech Review (TTR) are solely attributable to the authors of respective contributions. If these are contradictory to any particular person or entity, TTR shall not be liable for the present opinions, inadequacy of the information, any mistakes or inaccuracies.

Trinity Institute of Professional Studies
An ISO 9001:2008 Certified Institution
(Affiliated to Guru Gobind Singh Indraprastha University, Delhi)

Sector-9, Dwarka, New Delhi-110075
Ph: 45636921/22/23/24, Telefax : 45636925 www.tips.edu.in, tips@tips.edu.in

LIGHT TO ENLIGHTEN
TIPS

TRINITY INSTITUTE OF PROFESSIONAL STUDIES
Affiliated to Guru Gobind Singh Indraprastha University, Delhi)
“A+” Ranked Institution by SFRC, Govt. of NCT of Delhi.
Recognised under section 2(f) of the UGC Act, 1956
&
NAAC Accredited “B++” Grade Institution

STATEMENT ABOUT OWNERSHIP AND OTHER DETAILS OF TTR/TMR

FORM 5 (RULE 8)

1.	Printer's Name	:	Dr. R.K. Tandon
	Nationality	:	Indian
	Address	:	Trinity Institute of Professional Studies Sector-9, Dwarka, New Delhi 110075
2.	Place of Publication	:	Delhi
3.	Periodicity of Publication	:	Quarterly
4.	Publisher's Name	:	Dr. R.K. Tandon
	Nationality	:	Indian
	Address	:	Trinity Institute of Professional Studies Sector-9, Dwarka, New Delhi 110075
5.	Editor's Name	:	Dr. Vikas Rao Vadi
	Nationality	:	Indian
	Address	:	Trinity Institute of Professional Studies Sector-9, Dwarka, New Delhi 110075
6.	Name and Address of the individual who owns the journal and partners or shareholders holding more than one per cent of the capital.	:	CHAIRMAN Trinity Institute of Professional Studies Sector-9, Dwarka, New Delhi 110075
7.	Hosted at (url)	:	www.tips.edu.in

I, Dr. R.K. Tandon, hereby declare that the particulars given above are true to the best of my knowledge and belief.

Dr. R.K. Tandon

Merkle Hash Tree based Techniques for Cloud Data Integrity

Santosh Kumar Singh

One of the problems associated with outsourcing data to cloud service providers is the data integrity of outsourced data. Data integrity encompasses the completeness, correctness and freshness of the data. In the cloud storage framework, once clients remotely store their data on cloud storage providers, they will lose the physical control over their outsourced data. The risk of unauthorized access to the data increases dramatically. One of the most serious problems in cloud storage is to ensure the correctness of the outsourced data. Specifically, we need to protect these data from unauthorized operations; we also need to detect and recover users' data after unexpected changes. In this paper, we propose a publicly verifiable scheme to protect the integrity of cloud data, which is based on a Merkle hash tree. We adopt a three tuple to define the node of the new Merkle hash tree, which records the position of the corresponding node, so that users can verify the consistency of the challenge-response blocks by computing the root value directly without retrieving the whole Merkle hash tree.

Keywords: Cloud storage, Merkle Tree, PMT, Data Integrity, Database Security, Outsourced Data

1. **INTRODUCTION**

Data outsourcing means to store your data on third party cloud data service providers. It is cheaper and easier to maintain the data on a cloud data service instead of maintaining it in data owner's own premises. Besides all the benefits, data outsourcing poses numerous security threats to the outsourced data. The focus of this paper is data integrity that encompasses completeness, correctness and freshness. There are three parties involved in these schemes. Data owner (DO), data clients and data service provider (DSP). A DSP provides all the data services and can be trusted with the server availability, timely backups, replications and disaster recovery. But the DSP cannot be trusted with the integrity of outsourced data. A DSP has unlimited access to the data to make it possible for the DSP to forge the data in anyway.

In this paper, we present a new publicly verifiable scheme to ensure the integrity protection of remote cloud data. Our approach is based on a position-aware Merkle tree (PMT). The key benefit of our position-aware Merkle tree is that each node of the tree is aware of the relative position to its parent nodes. Therefore, the integrity verification phase in our approach does not need to retrieve the complete Merkle tree. To achieve this, we adopt a 3-tuple to define the node of the Merkle tree. The 3-tuple vector records the position of the corresponding node and user can verify the consistency of the challenge-response blocks by computing the root value directly (no need to get the whole Merkle tree back). Our approach supports unlimited verification challenges as well. In summary, we made the following contributions in this paper: – We propose a new data structure, position-aware Merkle tree, to support efficient integrity checking of cloud storage. The well-designed Merkle tree ensures that every node is sealed with its relative position information to its parent node. As a result, it may not be necessary to retrieve the whole tree structure to compute the root node; – We develop a new publicly verifiable scheme to check cloud data integrity based on the position-aware Merkle tree, which supports dynamic data operations effectively.

2 System model

We describe the system model shown in Fig. 1 for dynamic cloud data integrity verification, which is the classic model in cloud data integrity checking [4].

The cloud data integrity checking architecture usually consists of following parties:

- Cloud service provider (CSP) Cloud service providers have a cluster of the software and hardware resources, and provide flexible online computing and data storing services.
- Users outsource their data to the remote cloud storage to save the storing cost and utilize the computation resources provided by the service provider.
- Third-party authority (TPA) (optional) the third-party authority is an optional entity that represents a reliable, partially trusted, and independent entity that can offer audit and arbitration if needed.

Our position-aware Merkle-tree-based approach for dynamic integrity checking consists of two phases: Setup, Challenge-Prove.

Phase I (Setup) The Setup phase is a series of operations at the client side to initialize the system, including following functions:

1. KeyGen(1K) →{sk,pk} is a probabilistic key generation algorithm taking security parameter k as its input. The outputs are a public key pk and a private key sk. The client publishes pk and keeps sk as a secret.

2. TagGen(sk, pk, M) → {ϕ, metadata} takes the client's file M, pk, sk as its inputs and the outputs are M's tag ϕ and the metadata, which will be stored locally by the client. File M and the corresponding tag ϕ will be sent by clients and remotely stored at the server side. The metadata might be kept by the data owner or stored at the server side after signed by the owner.

Phase II (Challenge-prove) The Challenge-prove phase is an interaction procedure between the client and the server. The client calculates challenges and sends them to the server. The server computes the corresponding responses and replies the output to the client to prove its honesty. Phase II consists of following operations:

1. GenChallenge(s) → {chal} takes the client's private parameter s as the input and outputs challenge chal for the future query.

2. GenProof(gs , M, ϕ, chal) → {P} takes the user's public parameter gs, file M, metadata ϕ and challenge chal as its inputs and outputs the evidence P for the user to verify that the server possesses the outsourced file correctly.

3. CheckProof(pk, chal, metadata, P) → {"accept", "reject"} is the procedure to verify the server's possession of the target files. It takes the user's public key pk, challenge generated by client chal, metadata and evidence P as inputs. If the evidence P passed the verification, the function outputs "accept"; otherwise, CheckProof outputs "reject."

2.2 Merkle hash tree

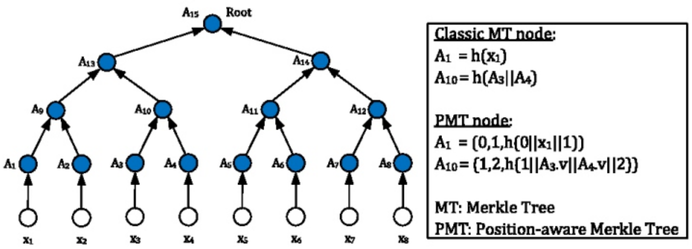


Fig. 2 Merkle hash tree vs. Position-aware Merkle tree

Merkle hash tree [10] is a popular technique for data integrity checking. A Merkle hash tree is a tree in which every non-leaf node is labelled as the hash value of its children nodes, and every leaf node is labelled as the hash value of a data block. There is a root on the top of the Merkle hash tree. Figure 2 illustrates a typical Merkle tree structure that contains eight leaf nodes, MT= {Ai |Ai = h(xi), 1 ≤ i ≤ 15}, where h() represents a hash function, e.g., SHA-1 [11], etc. The value of the non-leaf node Ai is h(A il || Ai r), where Ai l and Ai r represent Ai 's left child and right child, respectively. The root node of the MT is labelled as Aroot. Given a node Ai, the smallest ordered node set Ωi = {Ai1 >> Ai2 >> · · · } that can be used by Ai to compute the root node Aroot is called auxiliary authentication information (AAI). For example, in Fig. 2, the AAI of the node A2 is Ω2 = {A1 >> A10 >> A14}. In the previous Merkle-tree-based PDP scheme [5], it verifies the correctness of the queried file block mi 's tag, xi , using the auxiliary authentication information (AAI) Ωi . However, the server may cheat the client by returning another valid pair of data and AAI, {x'i , Ω'i }, to be verified. The client can compute the correct root node value using {x'i, Ω'i}, and the dishonest server may pass the validation without returning the correct response. Without the knowledge of the Merkle tree's structure, the client cannot validate whether the returned x'i is the corresponding tag of the required file block mi. One solution discussed in [5] is to publish the whole Merkle tree that user may access and retrieve it on-demand. Obviously, this is very inefficient.

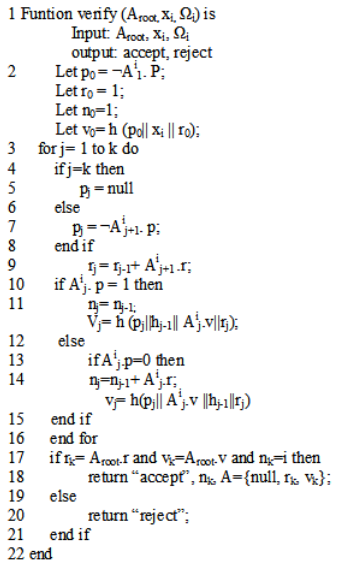
3 Design In this section, we introduce our position-aware Merkle tree. And we will propose a new efficient scheme for integrity verification supporting dynamic cloud data maintenance.

3.2 PMT-based data possession verification

In this subsection, we describe the data possession verification using PMT. Suppose the user only keeps the root node, Aroot = (Aroot.p, Aroot.r, Aroot.v), and the server keeps the outsourced file block sequence X = {x1, x2, . . . , xn}. If the user wants to check the integrity of her/his ith file block xi , she/he will send the request vector {i,"verify"}to the server and the server should return the corresponding integrity path {xi, Ωi }. The user executes Algorithm 1 (verify(Aroot,xi,Ωi) → {"accept","reject"}) to calculate the root node A'root based on the response {xi, Ωi } given by the server.

The user compares A'root with the original root Aroot that she/he kept locally. If Aroot = A'root, it means the server has sent the correct response.

As a result, the server passes the integrity verification and the verification algorithm outputs "accept", otherwise, the algorithm outputs "reject".



```
Funtion verify ($A_{root,} x_{i,} \Omega_i$) is
        Input: $A_{root}$, $x_i$, $\Omega_i$
        output: accept, reject
    Let $p_0 = \neg A^i_1. P$;
    Let $r_0 = 1$;
    Let $n_0$=1;
    Let $v_0$= h ($p_0$|| $x_i$ || $r_0$);
  for j= 1 to k do
    if j=k then
        $p_j$ = null
    else
        $p_j = \neg A^i_{j+1}. p$;
    end if
        $r_j = r_{j-1}+ A^i_{j+1}.r$;
    if $A^i_j$. p = 1 then
        $n_j= n_{j-1}$;
        $V_j$= h ($p_j$||$h_{j-1}$|| $A^i_j$.v||$r_j$);
    else
        if $A^i_j$.p=0 then
        $n_j=n_{j-1}+ A^i_j.r$;
          $v_j$= h($p_j$|| $A^i_j$.v ||$h_{j-1}$||$r_j$)
    end if
    end for
    if $r_k$= $A_{root}$.r and $v_k$=$A_{root}$.v and $n_k$=i then
        return "accept", $n_{k,}$ A={null, $r_{k,}$ $v_k$};
    else
        return "reject";
    end if
end
```

Algorithm 1: Integrity Verification Verify ()

5 Conclusion

In this paper, we propose a publicly verifiable scheme to support dynamic cloud data integrity protection based on a position-aware Merkle tree. We adopt a 3-tuple to define the node of the Merkle tree, which records the position of the corresponding node. The user can verify the consistency of the challenge-response blocks by computing the root value directly, and prevent the potential attack in Wang's scheme effectively. In our scheme, the storage complexity at the client side is O(1), the computation complexity at the client side is O(log n). The computation time of tag generation at the client side increases as the number of the file blocks increases. It will be a future work that identifies the optimal block size to balance the performance overhead between pre-processing and proof generation operation.

References

[1] DeswarteY, Quisquater J, SaidaneA(2003) Remote integrity checking. In: Conference on integrity and internal control in
Information systems, vol 03

[2] Gazzoni EL, Luiz D, Filho G, Sérgio P, Barreto LM, Politécnica E (2006) Demonstrating data possession and uncheatable data
transfer, 2006. IACR ePrint archive. Report 2006/150

[3] Ateniese G, Pietro D, Mancini L, TsudikG(2008) Scalable and efficient provable data possession. In: Proceedings of the 4th
international conference on security and privacy in communication netowrks, vol 9. ACM, New York

[4] Chris Erway C, KüpçüA, Papamanthou C, Tamassia R (2009) Dynamic provable data possession. In: Proceedings of the 16th
ACM conference on computer and communications security (CCS). ACM, New York, pp 213–222

[5] Wang Q, Wang C, Ren K, Lou W, Li J (2011) Enabling public verifiability and data dynamics for storage security in cloud
computing. IEEE Trans Parallel Distrib Syst 22(5):847–859

PALM VEIN TECHNOLOGY

UPASANA SINGH

Abstract

Palm vein technologies are one of the upcoming technologies which is highly secure. It is the world's first contactless personal identification system that uses the vein patterns in human palms to confirm a person's identity. It is highly secure because it uses information contained within the body and is also highly accurate because the pattern of veins in the palm is complex and unique to each individual. Moreover, its contact less feature gives it a hygienic advantage over other biometric authentication technologies.

Introduction

In the ubiquitous network society, where individuals can easily access their information anytime and anywhere, people are also faced with the risk that others can easily access the same information anytime and anywhere. Because of this risk, personal identification technology, which can distinguish between registered legitimate users and imposters, is now generating interest.

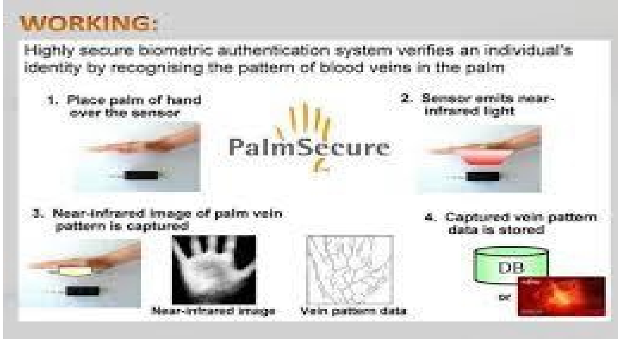
Currently, passwords, Personal Identification Numbers (4-digit PIN numbers) or identification cards are used for personal identification. However, cards can be stolen, and passwords and numbers can be guessed or forgotten.

Working

The palm secure works by capturing a person's vein pattern image while

radiating it with near-infrared rays. The Palm Secure detects the structure of the

pattern of veins on the palm of the human hand with the utmost precision. The sensor emits a near-infrared beam towards the palm of the hand and the blood flowing through these back to the heart with reduced oxygen absorbs this radiation, causing the veins to appear as a black pattern. This pattern is recorded by the sensor and is stored in encrypted form in a database, on a token or on a smart card. Veins are internal in the body and have wealth of differentiating features, assuming false identity through forgery is extremely difficult, thereby enabling an extremely high level of security. The Palm Secure technology is designed in such a way that it can only detect the vein pattern of living people.



WORKING:

Highly secure biometric authentication system verifies an individual's identity by recognising the pattern of blood veins in the palm

1. Place palm of hand over the sensor
2. Sensor emits near-infrared light
3. Near-infrared image of palm vein pattern is captured
4. Captured vein pattern data is stored

Figure 1: Working of palm vein pattern.

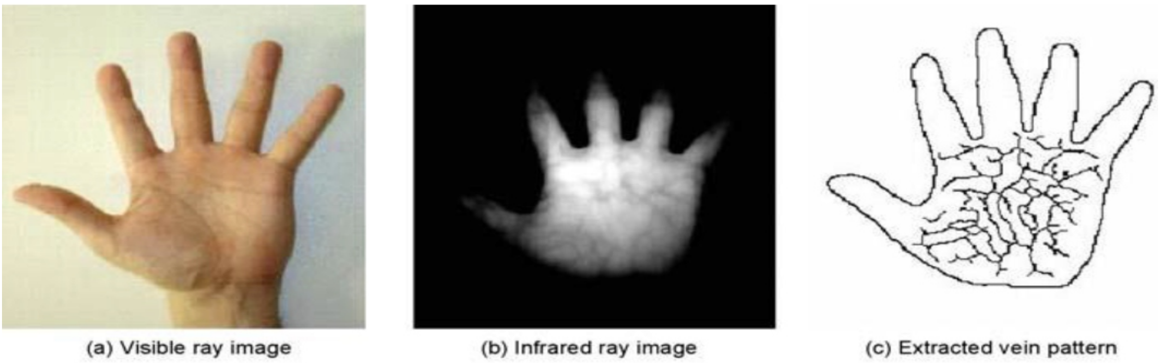
Technology

Palm vein authentication works by comparing the pattern of veins in the palm (which appear as blue lines) of a person being authenticated with a pattern stored in a database. Hemoglobin in the blood is oxygenated in the lungs and carries oxygen to the tissues of the body through the arteries. After it releases its oxygen to the tissues, the deoxidized hemoglobin returns to the heart through the veins. In vein authentication based on this principle, the region used for authentication is photographed with near-infrared light, and the vein pattern is extracted by image processing and registered. The vein pattern of the person being authenticated is then verified against the preregistered pattern.

Conclusion

This paper explains palm vein authentication. It is a palm-vein based authentication system that utilizes the latest in Biometric Security Technology. This technology is highly secure because it uses information contained within the body and is also highly accurate because

the pattern of veins in the palm is complex and unique to each individual. Moreover, its contactless feature gives it a hygienic advantage over other biometric authentication technologies.



(a) Visible ray image

(b) Infrared ray image

(c) Extracted vein pattern

Figure 2: Extracting a palm vein pattern.

Managing the Complexity of Today's Hybrid IT: Dealing with Security Gaps, Risks, and More

Shweta Sharma

With enterprises adding more capacity off premises in the public cloud, managed hosting, and colocation datacenters, it's no surprise that IT environments are becoming increasingly hybrid. A recent Voice of the Enterprise survey suggests that by 2019, less than half of all workloads will run on premises. While enterprise datacenters will continue to morph into larger facilities, many will still opt to operate on-premises, privately owned datacenters. And some outsourcing will continue. It's undeniable that hybrid IT environments offer many benefits, but their increased complexity creates security gaps, risk and a host of other issues.

Availability and Security Concerns

Organizations considering public cloud options face security, data sovereignty, service availability and latency concerns. Unused or underutilized cloud instances and workload-specific service requirements, including availability and security, could add to cloud costs. Some organizations insist that all net new applications be built for the cloud or delivered as a service. Others are updating existing workloads where possible. In short, organizations considering public cloud options have begun to address the concerns that directly affect their bottom line.

Establishing Business Strategies and Specific Goals

Managing hybrid IT environments will pose an even greater challenge as next-generation edge computing continues to grow. IoT and the distributed cloud will expand these boundaries, which, in turn, will boost demand for datacenter capacity. To run efficiently, hybrid IT environments need to spell out a business strategy and specific goals.

Evaluations must assess key factors per workload in addition to cost, including application performance and latency. The new hybrid must take into account business risk, as well as availability, redundancy and security concerns. An awareness of long-term goals must replace head-in-the-sand thinking when it comes efficiently managing hybrid IT environment

Maximizing DCIM to Address Hybrid Complexity

The increasing complexity of hybrid IT environments clearly underscores the importance of deploying some type of DCIM software.

This software can simplify things by providing visibility across datacenters, real-time monitoring, and capacity planning. Uniting data acquired from DCIM and IT systems management software with financial tools allows infrastructure managers to create standardized metrics and performance indicators for BEV (Business Enterprise Value) decisions.

Internal operational and business procedures and workflows must be updated to fully exploit the benefits of DCIM data and analysis. Dovetailing IT and facilities departments will help align IT demand with a datacenter's resources to improve capacity planning and management. It can also help with service provider performance reviews in the new hybrid IT environment.

Role-based information dashboards can also help present customized views for facility managers, IT managers, business line managers and executive management. Helping even further would be ongoing review processes to monitor how each venue meets established performance metrics.

Leveraging DCIM to Assess Workloads and Venues

Workload venues will shift based on current needs and infrastructure design. The right DCIM system can provide the real-time data an enterprise needs to assess location, infrastructure status, power, cooling and other pertinent data. Evaluating a center's BEV begins with a DCIM's ability to establish the cost effectiveness of a workload location. Is the location cost-effective for the work demanded of it? Could results be enhanced by moving to a cloud environment? Management and operations protocols will invariably differ from one datacenter location to the next. All the more reason for cost and efficiency considerations to follow standardized quantifiable metrics. This is needed to ensure accurate real-world comparisons across a specific hybrid environment.

How Social Media Could Shape the Future of Big Data

Diksha Hazrati

We're in the middle of the big data revolution. Companies are starting to gain access to more data than ever before, and data analysts are creating and using more sophisticated tools to make predictions about complex systems.

But the future of big data is being influenced by many variables—the hard limits of technological growth, supply and demand of data experts, business needs, and even consumer preferences. At the convergence point of these influences is one surprising sector, which could have a bigger role to play in the future of data than we previously could have imagined: social media.

Social Media's Influence

These are just some of the ways social media platforms could dictate the future of big data:

- Consumer data access. First, social media companies have access to enormous quantities of data. Our most popular apps have hundreds of millions of users, or in Facebook's case, more than a billion, and for each of those users, a platform has access to a history of personal posts, likes, interests, and demographic information. There are few other applications that have the potential to gather that much information about so many people, giving social media platforms far more potential for development in the future.
- Business tools. We also can't discount the ways that social media companies have made data analytics accessible to more businesses. Facebook tools give entrepreneurs and small business owners a way to learn in-depth features of their target audiences, and an intuitive platform for crunching the numbers. Statistical analysis and data projections once limited to the realm of data scientists and analysts have now become available to even the least experienced amateurs. Social platforms are incentivized to improve accessibility for other businesses, so it makes sense they would have some of the most innovative software.
- Access to resources. The biggest social media giants around today have tremendous access to resources, and influence to put those resources to good use. Facebook, for example, is now worth nearly half a trillion dollars. With an incentive to learn more about their customers and innovate new, exciting technologies, these companies already have the money and the talent necessary to make those visions a reality.
- Competition. The sheer number of social media apps is also a factor worth consideration. Facebook, Twitter, LinkedIn, Instagram(owned by Facebook), and Snapchat may be the frontrunners for now, but there will always be room for more major players. The competition has two major effects; first, the threat of companies operating in the same space forces each company to stay on top of its game. It encourages faster, more thorough innovation. Second, the number of progressing tech companies multiplies the amount of data and tools available to the public.
- Privacy concerns and regulations. The influence of social media over the future of data isn't just about accessibility; social media apps are also drawing attention to issues of consumer privacy, as evidenced by the latest in a long line of scandals. As consumers and policymakers learn more about how apps like Facebook collect and manage data, they've become increasingly concerned about regulation and protection. The EU and other governing bodies are moving to establish firmer policies on data rights, which could have long-lasting consequences for any business involved in big data.

BRAIN GATE

Neha Aggrawal

The mind-to-movement system that allows a quadriplegic man to control a computer using only his thoughts is a scientific milestone. It was reached, in large part, through the brain gate system. This system has become a boon to the paralyzed. The Brain Gate System is based on Cyber kinetics platform technology to sense, transmit, analyze and apply the language of neurons. The principle of operation behind the Brain Gate System is that with intact brain function, brain signals are generated even though they are not sent to the arms, hands and legs. The signals are interpreted and translated into cursor movements, offering the user an alternate Brain Gate pathway to control a computer with thought, just as individuals who have the ability to move their hands use a mouse. The 'Brain Gate' contains tiny spikes that will extend down about one millimetre into the brain after being implanted beneath the skull, monitoring the activity from a small group of neurons. It will now be possible for a patient with spinal cord injury to produce brain signals that relay the intention of moving the paralyzed limbs, as signals to an implanted sensor, which is then output as electronic impulses. These impulses enable the user to operate mechanical devices with the help of a computer cursor.

The 'Brain Gate' contains tiny spikes that will extend down about one millimetre into the brain after being implanted beneath the skull, monitoring the activity from a small group of neurons.It will now be possible for a patient with spinal cord injury to produce brain signals that relay the intention of moving the paralyzed limbs, as signals to an implanted sensor, which is then output as electronic impulses. These impulses enable the user to operate mechanical devices with the help of a computer cursor.

HOW DOES THE BRAIN CONTROL MOTOR FUNCTION?

The brain is "hardwired" with connections, which are made by billions of neurons that make electricity whenever they are stimulated. The electrical patterns are called brain waves. Neurons act like the wires and gates in a computer, gathering and transmitting electrochemical signals over distances as far as several feet. The brain encodes information not by relying on single neurons, but by spreading it across large populations of neurons, and by rapidly adapting to new circumstances.

Motor neurons carry signals from the central nervous system to the muscles, skin and glands of the body, while sensory neurons carry signals from those outer parts of the body to the central nervous system. Receptors sense things like chemicals, light, and sound and encode this information into electrochemical signals transmitted by the sensory neurons. And interneurons tie everything together by connecting the various neurons within the brain and spinal cord. The part of the brain that controls motor skills is located at the ear of the frontal lobe.

How does this communication happen? Muscles in the body's limbs contain embedded sensors called muscle spindles that measure the length and speed of the muscles as they stretch and contract as you move. Other sensors in the skin respond to stretching and pressure. Even if paralysis or disease damages the part of the brain that processes movement, the brain still makes neural signals. They're just not being sent to the arms, hands and legs.

A technique called neuron feedback uses connecting sensors on the scalp to translate brain waves into information a person can learn from. The sensors register different frequencies of the signals produced in the brain. These changes in brain wave patterns indicate whether someone is concentrating or suppressing his impulses, or whether he is relaxed or tense

NEURON PROSTHETIC DEVICE

Neuron prosthetic device known as Brain gate converts brain activity into computer commands. A sensor is implanted on the brain, and electrodes are hooked up to wires that travel to a pedestal on the scalp. From there, a fiber optic cable carries the brain activity data to a nearby computer.

PRINCIPLE

"The principle of operation of the BrainGate Neural Interface System is that with intact brain function, neural signals are generated even though they are not sent to the arms, hands and legs. These signals are interpreted by the System and a cursor is shown to the user on a computer screen that provides an alternate "BrainGate pathway". The user can use that cursor to control the computer, Just as a mouse is used."

Brain Gate is a brain implant system developed by the bio-tech company Cyber kinetics in 2003 in conjunction with the Department of Neuroscience at Brown University. The device was designed to help those who have lost control of their limbs, or other bodily functions, such as patients with amyotrophic lateral sclerosis (ALS) or spinal cord injury. The computer chip, which is implanted into the patient and converts the intention of the user into computer commands. Currently the chip uses 100 hair-thin electrodes that 'hear' neurons firing in specific areas of the brain, for example, the area that controls arm movement. The activity is translated into electrically charged signals and is then sent and decoded using a program, which can move either a robotic arm or a computer cursor. According to the Cyberkinetics' website, three patients have been implanted with the Brain gate system. The company has confirmed that one patient (Matt Nagle) has a spinal cord injury, whilst another has advanced ALS. In addition to real-time analysis of neuron patterns to relay movement, the Brain gate array is also capable of recording electrical data for later analysis. A potential use of this feature would be for a neurologist to study seizure patterns in a patient with epilepsy.

WORKING

Operation of the BCI system is not simply listening the EEG of user in a way that let's tap this EEG in and listen what happens. The user usually generates some sort of mental activity pattern that is later detected and classified.

PREPROCESSING

The raw EEG signal requires some preprocessing before the feature extraction. This preprocessing includes removing unnecessary frequency bands, averaging the current brain activity level, transforming the measured scalp potentials to cortex potentials. Frequency bands of the EEG:

DETECTION

The detection of the input from the user and them translating it into an action could be considered as key part of any BCI system. This detection means to try to find out these mental tasks from the EEG signal. It can be done in time-domain, e.g. by. Comparing amplitudes of the EEG and in frequency-domain. This involves usually digital signal processing for sampling and band pass filtering the signal, then calculating these time -or frequency domain features and then classifying them. These classification algorithms include simple comparison of amplitudes linear and nonlinear equations and artificial neural networks. By constant feedback from user to the system and vice versa, both partners gradually learn more from each other and improve the overall performance.

CONTROL

The final part consists of applying the will of the user to the used application. The user chooses an action by controlling his brain activity, which is then detected and classified to corresponding action. Feedback is provided to user by audio-visual means e.g. when typing with virtual keyboard, letter appears to the message box etc.

CONCLUSION

The idea of moving robots or prosthetic devices not by manual control, but by mere "thinking" (i.e., the brain activity of human subjects) has been a fascinated approach. Medical cures are unavailable for many forms of neural and muscular paralysis. The enormity of the deficits caused by paralysis is a strong motivation to pursue BMI solutions. So this idea helps many patients to control the prosthetic devices of their own by simply thinking about the task.

This technology is well supported by the latest fields of Biomedical Instrumentation, Microelectronics; signal processing, Artificial Neural Networks and Robotics which has overwhelming developments. Hope these systems will be effectively implemented for many Bio-medical applications.

Design of a Framework for Predictive Analytics of Crime using Data Mining

Shruti Bhalla

India is a vast country with diversified societies. Security is considered to be one of the major concerns and the issue is continuing to grow in intensity and complexity. Security is an aspect that is given top priority by all political and government worldwide and are aiming to reduce crime incidence .

Crime is neither systematic nor entirely random. The Oxford English Dictionary defines crime simply as: 'An action or omission which constitutes an offence and is punishable by law'. The Oxford Dictionary of Sociology defines crime in a more complex way: 'an offence which goes beyond the personal and into the public sphere, breaking prohibitory rules or laws, to which legitimate punishments are attached, and which requires the intervention of a public authority.'

Criminology is a discipline that focuses on:

- The study of crime
- The study of those who commit crime
- The study of the criminal justice and penal (punishment) system

Criminology is an area that focuses the scientific study of crime and criminal behavior and law enforcement and is a process that aims to identify crime characteristics. Crime analysis, a part of criminology, is a task that includes exploring and detecting crimes and their relationships with criminals (Levine, N., 2002). It is one of the most important fields where the application of data mining techniques can produce important results. Governments deal with large amount of data related to crime.

In the present scenario, the criminals are becoming technologically sophisticated in committing crimes (Amarnathan, 2003). Therefore, police need such a crime analysis tool to catch criminals and to remain ahead in the eternal race between the criminals and the law enforcement. The police should use the current technologies (Corcoran et al., 2003; Ozkan, 2004) to give themselves the much-needed edge. Availability of relevant and timely information is of utmost necessity in conducting of daily business and activities by the police, particularly in crime investigation and detection of criminals.

- The data available is inconsistent and are incomplete thus making the task of formal analysis a far more difficult.
- Investigation of the crime takes longer duration due to complexity of issues.

Most law enforcement agencies today are faced with large volume of data that must be processed and transformed into useful information (Brown, 2003). Data mining can greatly improve crime analysis and aid in reducing and preventing crime.

Some of the techniques of data mining are:

- Neural Networks: Neural Networks are well suited to tackle problems that people are good at solving like predictions and pattern recognition.
- Rule Induction: The extraction of useful if-then rules from data based on statistical significance.
- Decision Trees: Tree shaped structures that represent set of decisions. These decisions generate rules for the classification of the data set.

Choosing the best algorithm to use for a specific task can be a challenge. While we can use different algorithms to perform the same task, each algorithm produces a different result, and some algorithms can produce more than one type of result.

ANN for Node Localization in Wireless Sensor Network

Shikha Bhalla

With the increasing use and application of Wireless Sensor Networks (WSN), need has arisen to make them more efficient in a cost effective way. An important area which can bring efficiency to WSNs is the localization process by which the sensor nodes in the network can identify their own location in the overall network.A Wireless Sensor Network is an interconnected network of multiple sensor nodes, which communicate with each other to create a smart sensor network which performs various functions. The role of sensor nodes is to convert the physical conditions (e.g. temperature, atmospheric pressure, humidity etc.) surrounding them to electric signals. These signals are then transmitted in the entire network in a fashion that each sensor node co-operates and communicates with each other. The data being so transmitted through signals is centrally collated and analyzed by few special nodes (often known as base station nodes).These anchor nodes provide the useful information about the area covered by WSN. These WSNs are now increasingly being used to provide critical and sometimes lifesaving information about the environment e.g. providing early warning of floods, cyclones, Tsunami etc. Apart from these, such networks also have practical usage in other areas like industrial, commercial, military operations etc. Many of these applications require the precise information about the location of sensor node in the network for tasks such as network routing, communication and to state geographical source of events such as fire detection, earthquake detection, flood detection, temperature monitoring etc. This phenomenon is achieved by a process called Localization, wherein the node placed in a network determines its own location in relation to the anchor nodes. The general approach used to facilitate the localization is to deploy certain nodes which are aware of their location in the overall network and are called anchor nodes (or Beacon nodes). The other nodes in the system calculate the

distance between their location and the anchor nodes. There are quite a few techniques to enable the process of localization which can be broadly classified into a) range based; and b) range free techniques [4]. In a range based technique, absolute distance or absolute angle is measured between the two nodes using methodologies like ToA (Time of Arrival), TDoA (Time-Difference of Arrival), AoA (Angle of arrival), and RSS (Received signal strength).On the contrary, range free techniques rely on the connectivity and proximity of nodes viz-a-viz the anchor nodes to estimate the distance between them. These estimates are based on certain parameters like amount of packets transferred during routing etc. Range based techniques are more precise and accurate than range free techniques however the latter are more simple and cost effective. These days, the range-free techniques are gaining more popularity than the range-based methods. Application of Artificial Vol 4 Issue 1 Page 19
neural network (ANN) as a range free technique is one of the forthcoming methods that can be used for localization in WSNs