Information Regarding Principal Investigator

Name: ANKAN HORE
Date of Birth: 2001-11-11
Contact Number: 2147483647
E-mail Id: ankanhore238@gmail.com
Biodata File: File Uploaded Click to view file
Designation: Student
Residential Address: 221 Baker Street

Information Regarding Institution of Principal Investigator

Institution Name: Institute of Engineering & Management, Kolkata
Department: IT
Address of the Institution: Gurukul, Y-12, Block -EP,
Salt Lake Electronics Complex, Sector V,
Salt Lake Sec 5

Brief Description of the Project

Title: Clinical Research in Homoeopathy helps in generating, validating and consolidating scientific evidences (in terms of safety, efficacy and effectiveness) of homoeopathic medications, procedures and treatment regimes. These researches may be useful in in prevention, treatment of various diseases, decision making for stake holders and thus help in improving clinical care. The aim is to carry out evidence based trials based on modern scientific parameters (double blinding; objective assessment criteria, statistical analysis, etc.) without conflicting with the doctrines of Homoeopathy. More emphasis is laid upon the clinical evaluation of homoeopathic medicines in disease conditions of national health importance, where no curative treatment is available in conventional medicine; endemic diseases in certain parts of the country and the so called surgical disease

Aims and Objectives: Network security problems can be divided roughly into four closely intertwined areas: secrecy, authentication, nonrepudiation, and integrity control. Secrecy, also called confidentiality, has to do with keeping information out of the hands of unauthorized users. This is what usually comes to mind when people think about network security. Authentication deals with determining whom you are talking to before revealing sensitive information or entering into a business deal. Nonrepudiation deals with signatures. Message Integrity: Even if the sender and receiver are able to authenticate each other, they also want to insure that the content of their communication is not altered, either maliciously or by accident, in transmission. Extensions to the checksumming techniques that we encountered

Introduction: Network security problems can be divided roughly into four closely intertwined areas: secrecy, authentication, nonrepudiation, and integrity control. Secrecy, also called confidentiality, has to do with keeping information out of the hands of unauthorized users. This is what usually comes to mind when people think about network security. Authentication deals with determining whom you are talking to before revealing sensitive information or entering into a business deal. Nonrepudiation deals with signatures. Message Integrity: Even if the sender and receiver are able to authenticate each other, they also want to insure that the content of their communication is not altered, either maliciously or by accident, in transmission. Extensions to the checksumming techniques that we encountered in reliable transport and

data link protocols. Cryptography is an emerging technology, which is important for network security. The widespread use of computerised data storage, processing and transmission makes sensitive, valuable and personal information vulnerable to unauthorised access while in storage or transmission. Due to continuing advancements in communications and eavesdropping technologies, business organisations and private individuals are beginning to protect their information in computer systems and networks using cryptographic techniques, which , until very recently, were exclusively used by the military and diplomatic communities.

Review of literature: Network security problems can be divided roughly into four closely intertwined areas: secrecy, authentication, nonrepudiation, and integrity control. Secrecy, also called confidentiality, has to do with keeping information out of the hands of unauthorized users. This is what usually comes to mind when people think about network security. Authentication deals with determining whom you are talking to before revealing sensitive information or entering into a business deal. Nonrepudiation deals with signatures. Message Integrity: Even if the sender and receiver are able to authenticate each other, they also want to insure that the content of their communication is not altered, either maliciously or by accident, in transmission. Extensions to the checksumming techniques that we encountered in reliable transport and data link protocols. Cryptography is an emerging technology, which is important for network security. The widespread use of computerised data storage, processing and trans

Abstract & Keywords of the Project

Abstract: Network Security & Cryptography is a concept to protect network and data transmission over wireless network. Data Security is the main aspect of secure data transmission over unreliable network. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. In this paper we also studied cryptography along with its principles. Cryptographic systems with ciphers are described. The cryptographic models and algorithms are outlined.

Keywords: cryptography

Information Regarding Coinvestigators (if any)

Co-Investigator 1
Name: TKH
Designation: asst prof
Email-id: tkh123@gmail.com
Address: Gurukul, Y-12, Block -EP,
Salt Lake Electronics Complex, Sector V,

Biodata: File Uploaded Click to view file Information Regarding Collaborating Institute (if any)
Name of the Institution: IEM
Postal Address: Gurukul, Y-12, Block -EP,
Salt Lake Electronics Complex, Sector V,
Telephone Number: 0332357296
Fax Number: 33333333
E-mail Id: iemcal@gmail.com Ethics Committee
Name of the ethics committee: Ethics Comm
Approval Status: In review
Approval Date: 2017-12-12
Approval File: File Uploaded Click to view file Duration of Research Project
Period required for pre-trial preparations: 10 months
Period that may be required for analysing the data: 10 months
Period which may be needed for collecting the data: 10 months
Methodology
Study Type: Post Graduate
Study Design: Non-randomized, Placebo Controlled Trial
Method for Allocation of Concealment: Dates of Birth or day of the week
Target Sample Size: 1000
Date of First Enrollment: 2016-01-01
Estimated duration of subject participation: 2 years
Type of trial: Interventional
Method of Blinding/Masking: Open Label
Phase of Trial: Phase 1, Phase 2
Method for Generating Randomization Sequence: Shuffling Card
Description of the sequence and duration of all trial periods: users. This is what usually comes to mind when people think about network security. Authentication deals with determining whom you are talking to before revealing sensitive information or entering into a business deal. Nonrepudiation deals with signatures. Message Integrity: Even if the sender and receiver are able to authenticate each other, they also want to insure that the content of their communication is not altered, either malicously or by accident, in transmission. Extensions to the checksumming techniques that we encountered in reliable transport and data link protocols. Cryptogra
Follow Up, if any: users. This is what usually comes to mind when people think about network security. Authentication deals with determining whom you are talking to before revealing sensitive information or entering into a business deal. Nonrepudiation deals with signatures. Message Integrity: Even if the sender and receiver are able to authenticate each other, they also want to insure that the content of their communication is not altered, either malicously or by accident, in transmission. Extensions to the Intervention
Description of, and justification for, the route of administration, dosage, dosage regimen, and treatment period(s): Network security problems can be divided roughly into four closely intertwined areas: secrecy, authentication,
nonrepudiation, and integrity control. Secrecy, also called confidentiality, has to do with keeping information out of the hands
of unauthorized users. This is what usually comes to mind when people think about network security. Authentication deals with

determining whom you are talking to before revealing sensitive information or entering into a business deal. Nonrepudiation
deals with signatures. Message Integrity: Even if the sender and receiver are able to authenticate each ot
A description of the trial treatment(s) and the dosage and dosage regimen of the investigational product(s). Also include a description of the dosage form, packaging and labelling of the investigational product(s): Network security problems can be divided roughly into four closely intertwined areas: secrecy, authentication,
nonrepudiation, and integrity control. Secrecy, also called confidentiality, has to do with keeping information out of the hands
of unauthorized users. This is what usually comes to mind when people think about network security. Authentication deals with
determining whom you are talking to before revealing sensitive information or entering into a business deal. Nonrepudiation
deals with signatures. Message Integrity: Even if the sender and receiver are able to authenticate each ot
A description of the “stopping rules” or “discontinuation criteria” for individual subjects, parts of trial and entire trial: Network security problems can be divided roughly into four closely intertwined areas: secrecy, authentication,
nonrepudiation, and integrity control. Secrecy, also called confidentiality, has to do with keeping information out of the hands
of unauthorized users. This is what usually comes to mind when people think about network security. Authentication deals with
determining whom you are talking to before revealing sensitive information or entering into a business deal. Nonrepudiation
deals with signatures. Message Integrity: Even if the sender and receiver are able to authenticate each ot Subject withdrawal criteria i.e. terminating investigational product treatment/trial treatment and procedures specifying
When and how to withdraw subjects from the trial/investigational product treatment: Due to continuing advancements in communications and eavesdropping technologies, business organisations and
private individuals are beginning to protect their information in computer systems and networks using cryptographic techniques,
which , until very recently, were exclusively used by the military and diplomatic communities.
The type and timing of the data to be collected for withdrawn subjects : Due to continuing advancements in communications and eavesdropping technologies, business organisations and
private individuals are beginning to protect their information in computer systems and networks using cryptographic techniques,
which , until very recently, were exclusively used by the military and diplomatic communities.
Whether and how subjects are to be replaced : which , until very recently, were exclusively used by the military and diplomatic communities.
The follow-up for subjects withdrawn from investigational product treatment/trial treatment: which , until very recently, were exclusively used by the military and diplomatic communities. Assessment of safety of trial subjects/research participants Assessment of safety of trial subjects/research participants: which , until very recently, were exclusively used by the military and diplomatic communities.

The methods and timing for assessing, recording, and analysing safety parameters: which , until very recently, were exclusively used by the military and diplomatic communities.
Procedures for eliciting report of and for recording and reporting adverse event and intercurrent illnesses : which , until very recently, were exclusively used by the military and diplomatic communities.
The type and duration of the follow-up of subjects after adverse events: which , until very recently, were exclusively used by the military and diplomatic communities. Journal Journal 1
Author's Name: jour auth name
Title of the article: jour title
Abbreviated Title of Journal: hour abb title
Date of publication: 2014/05
Volume Number : 6
Issue Numbers: 2
Page Number(s): 239,435,53,55 Books Books 1
Author's Name: book auth name
Title of Book: book title
Edition: 9th
Place of Publication: book pub place
Publisher: book pub
Year of Publication: 2015 Govt. and Technical Reports Reports 1
Author's Name/Organisation Name: rep auth name
Title of Report: rep title
Place of Publication: rep pub place
Publisher: rep pub
Date of Publication: 2007
Total Number of Pages: 5
Report Number: 59 Websites and Social Media Websites and Social Media 1
Author/Organisation Name: web author
Title of the Page: web title
Place of Publication: web place pub
Publisher: web pub
Date/Year of Publication: 20/7/2014 Secondary Sources - Thesis/Dissertation Secondary Sources - Thesis/Dissertation 1
Author's Name: Ss auth name
Title of Thesis: thesis title
Place of Publication: ss place pub
Publisher: ss publisher
Year of Publication: 2007
Number of Pages: 78 Newspaper Newspaper 1
Author's Name: newspaper name
Title of Article: news title
Newspaper Title: news title
Place of Publication: news pub place
Date of Publication: 15/04/2001
Section: news sec
Location: news loc
Cited On: 2004 03 01 Encyclopedia Encyclopedia 1
Author's Name: enc auth name
Title of encyclopedia: anc title

Place of Publication: enc pub place
Publisher: enc pub
Year of Publication: 2009
Title of Article: enc art title
Page Number: 300

Statistics

A description of the statistical methods to be employed, including timing of any planned interim analysis: Network Security is the most vital component in information security because it is responsible for securing all information passed through networked computers. Network Security refers to all hardware and software functions, characteristics, features, operational procedures, accountability, measures, access control, and administrative and management policy required to provide an acceptable level of protection for Hardware and Software , and information in a network.

The number of subjects planned to be enrolled. In multi-centre trials, the numbers of enrolled subjects projected for each trial site should be specified. Reason for choice of sample size, including reflections on (or calculations of) the power of the trial and clinical justification: Network Security is the most vital component in information security because it is responsible for securing all information passed through networked computers. Network Security refers to all hardware and software functions, characteristics, features, operational procedures, accountability, measures, access control, and administrative and management policy required to provide an acceptable level of protection for Hardware and Software , and information in a network.

The level of significance to be used: Network Security is the most vital component in information security because it is responsible for securing all information passed through networked computers. Network Security refers to all hardware and software functions, characteristics, features, operational procedures, accountability, measures, access control, and administrative and management policy required to provide an acceptable level of protection for Hardware and Software , and information in a network.

Criteria for the termination of the trial: Network Security is the most vital component in information security because it is responsible for securing all information passed through networked computers. Network Security refers to all hardware and software functions, characteristics, features, operational procedures, accountability, measures, access control, and administrative and management policy required to provide an acceptable level of protection for Hardware and Software , and information in a network.

Procedure for accounting for missing, unused, and spurious data : Network Security is the most vital component in information security because it is responsible for securing all information passed through networked computers. Network Security refers to all hardware and software functions, characteristics, features, operational procedures, accountability, measures, access control, and administrative and management policy required to provide an acceptable level of protection for Hardware and Software , and information in a network.

Procedures for reporting any deviation(s) from the original statistical plan: Network Security is the most vital component in information security

because it is responsible for securing all
information passed through networked computers. Network Security refers to all hardware and software functions,
characteristics, features, operational procedures, accountability, measures, access control, and administrative and management
policy required to provide an acceptable level of protection for Hardware and Software , and information in a network.
The selection of subjects to be included in the analysis : Network Security is the most vital component in information security because it is responsible for securing all
information passed through networked computers. Network Security refers to all hardware and software functions,
characteristics, features, operational procedures, accountability, measures, access control, and administrative and management
policy required to provide an acceptable level of protection for Hardware and Software , and information in a network. Summary
Summary of the proposed research Project/Synopsis : Network Security is the most vital component in information security because it is responsible for securing all
information passed through networked computers. Network Security refers to all hardware and software functions,
characteristics, features, operational procedures, accountability, measures, access control, and administrative and management
policy required to provide an acceptable level of protection for Hardware and Software , and information in a network. Budget
Recurring Expenditure Salary Justification 1st Year 2nd Year 3rd Year Total
1 7637 6467 3453 7378 17298 Non-Recurring Expenditure Equipment
Justification 1st Year 2nd Year 3rd Year Total
1 3435 2627 7388 4336 14351 Non-Recurring Expenditure Heading
Justification 1st Year 2nd Year 3rd Year Total
books 4236 3546 3383 9807
tada 3534 8723 6368 18729
instsupport 3536 2767 8237 15149
feeofPI 4356 7356 8822 26006
misc 2568 5515 7737 15915
expenses 4246 5525 7728 22091