IORD Journal of Science & Technology
E-ISSN: 2348-0831
Volume 3, Issue 3 (MAR-APRIL 2017) PP93 -98
IMPACT FACTOR 1.719
www.iord.in

"To Detecting provenance Forgery & packet drop attacks by using Statistical method algorithm"

Miss. Kanchan Gawande [2]

[1](PG Student,VITNagpur)

Abstract- ***Many application domains, such as real-time financial analysis, e-healthcare systems, sensor networks, are characterized by continuous data streaming from multiple sources and through intermediate processing by multiple aggregators. Keeping track of data provenance in such highly dynamic context is an important requirement, since data provenance is a key factor in assessing data trustworthiness which is crucial for many applications. Provenance management for streaming data requires addressing several challenges, including the assurance of high processing throughput, low bandwidth consumption, storage efficiency and secure transmission. In this paper, we propose a novel approach to securely transmit provenance for streaming data (focusing on sensor network) by embedding provenance into the interpacket timing domain while addressing the above mentioned issues. As provenance is hidden in another host-medium, our solution can be conceptualized as watermarking technique. However, unlike traditional watermarking approaches, we embed provenance over the interpacket delays (IPDs) rather than in the sensor data themselves, hence avoiding the problem of data degradation due to watermarking. Provenance is extracted by the data receiver utilizing an optimal threshold-based mechanism which minimizes the probability of provenance decoding errors. The resiliency of the scheme against outside and inside attackers is established through an extensive security analysis. Experiments show that our technique can recover provenance up to a certain level against perturbations to inter-packet timing characteristics***.

Keywords— (Existing system Encryption Technique,Proposed system,feature Application)

1. INTRODUCTION

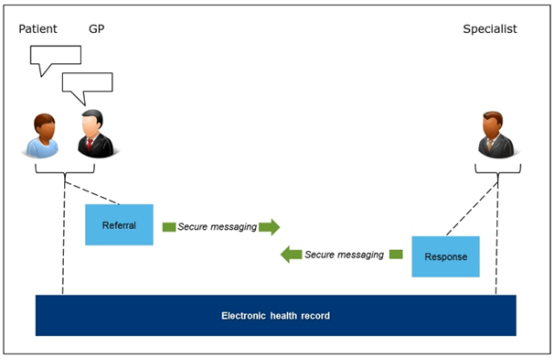
Light weight secure system. SENSOR networks are used in numerous application domains, such as cyberphysical infrastructure systems, environmental monitoring, power grids, etc. Data are produced at a large number of sensor node sources and processed in-network at intermediate hops on their way to a base station (BS) that performs decision-making. The diversity of data sources creates the need to assure the trustworthiness of data, such that only trustworthy information is considered in the decision process. Data provenance is an effective method to assess data trustworthiness, since it summarizes the history of ownership and the actions performed on the data. The application will contain secured messaging between two web based accounts, where 2 users will be able to get login to the application and check the messages between each other also can send messages to each other. The messages will be so secured that no one will be able to read the messages with our particular authority.

2. Existing Systems

Existing Systems in php to send message from one user to another user don't uses encryptions and messages are sent directly from one user to another. These types of systems are not secured and can be easily hacked. We addressed the problem of securely transmitting provenance for sensor networks, and proposed a light-weight provenance encoding and decoding scheme based on Bloom filters. The scheme ensures confidentiality, integrity and freshness of provenance. We extended the scheme to incorporate data-provenance binding, and to include packet sequence information that supports detection of packet loss attacks. Experimental and analytical evaluation results show that the proposed scheme is effective, light-weight and scalable. In future work, we plan to implement a real system prototype of our secure provenance scheme, and to improve the accuracy of packet loss detection, especially in the case of multiple

consecutive malicious sensor nodes. The economic basis for making standards is the concept we call a natural monopoly. This means (at least in this context) that a successful standard will attract and hold all users. Currency is an example: when the state decrees that we will all use a particular currency unit, this becomes a monolpoly. Possessing any other currency means you can't trade, or only at a penalty.

Below image Explains Traditional messaging system.



Similar natural monopolies would be rail transport, electricity, phones, the Internet Protocol. You want your toaster to plug into any power socket. You want your phone to reach anyone and be reachable by anyone.

When a successful natural monopoly emerges, thanks to luck or regulation or market forces, it eliminates a lot of waste, also called "friction costs", "transaction costs", or perhaps "excess profits". Natural monopolies can create huge value. Vendors, those selling stuff, have a corresponding incentive to try to capture that value, restoring the profits that would be lost by too much of Adam Smith's invisible hand. The natural monopoly can benefit users, by releasing value. A good example: the Internet. But it can also punish them, by capturing them and then taxing them without mercy. Your mobile phone bill is a case in point.

3. Existing Work

Pedigree [26] captures provenance for network packets in the form of per packet tags that store a history of all nodes and processes that manipulated the packet. However, the scheme assumes a trusted environment which is not realistic in sensor networks. ExSPAN [27] describes the history and derivations of network state that result from the execution of a distributed protocol. This system also does not address security concerns and is specific to some network use cases. SNP [28] extends network provenance to adversarial environments. Since all of these systems are general purpose network provenance systems, they are not optimized for the resource constrained sensor networks. Hasan et al. [5] propose a chain model of provenance and ensure integrity and confidentiality through encryption, checksum and incremental chained signature mechanism. Syalim et al. [29] extend this method by applying digital signatures to a DAG model of provenance. However, these generic solutions are not aware of the sensor network specific assumptions, constraints, etc. Since provenance tends

4. Proposed System

The Project is secured chat system, where encryption is done using cyphertext with autogenerated salt for each message. End to end encryption and dycryption is done so that message will be complete secure. The encrypted message can be decrypted for particular user only using particular decryption unique key for each message.

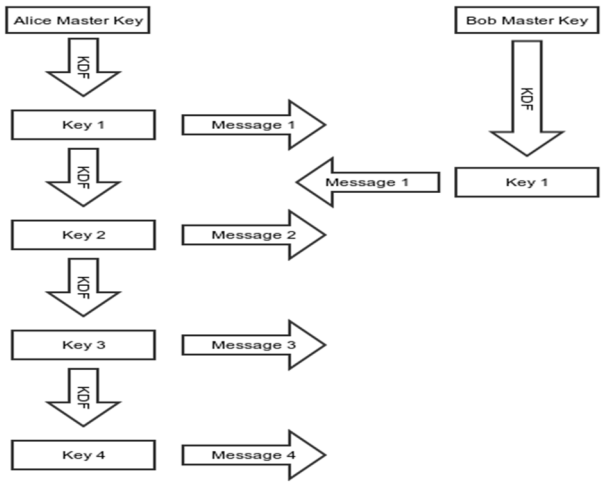
In cryptography, ciphertext or cyphertext is the result of encryption performed on plaintext using an algorithm, called a cipher.Ciphertext is also known as encrypted or encoded information because it contains a form of the original plaintext that is unreadable by a human or computer without the proper cipher to decrypt it. Decryption, the inverse of encryption, is the process of turning ciphertext into readable plaintext. Ciphertext is not to be confused with codetext because the latter is a result of a code, not a cipher.

Cryptanalysis is the study of methods for obtaining the meaning of encrypted information, without access to the

secret information that is normally required to do so. Typically, this involves knowing how the system works and finding a secret key. Cryptanalysis is also referred to as codebreaking or cracking the code. Ciphertext is generally the easiest part of a cryptosystem to obtain and therefore is an important part of cryptanalysis. Depending on what information is available and what type of cipher is being analyzed, crypanalysts can follow one or more attack models to crack a cipher.

5. New Features in the application

The application contains login of super admin who can create users which then can send messages to each other. The message is encrypted from one user and can be sent over to another user, at the other end message gets decrypted.



End to end encryption will be used in this application to make it secure it in all the ways. We will use socket for realtime communication or messaging.We consider a multihop wireless sensor network, consisting of a number of sensor nodes and a base station that collects data from the network

6. Methodology USED

Technologies Used to create the application:

1) PHP

PHP is a server-side scripting language designed primarily for web development but also used as a general-purpose programming language. Originally created by Rasmus Lerdorf in 1994 the PHP reference implementation is now produced by The PHP Development Team PHP originally stood for Personal Home Page, but it now stands for the recursive acronym PHP: Hypertext Preprocessor.

PHP code may be embedded into HTML or HTML5 markup, or it can be used in combination with various web template systems, web content management systems and web frameworks. PHP code is usually processed by a PHP interpreter implemented as a module in the web server or as a Common Gateway Interface (CGI) executable. The web server software combines the results of the interpreted and executed PHP code, which may be any type of data, including images, with the generated web page. PHP code may also be executed with a command-line interface (CLI) and can be used to implement standalone graphical applications.

The standard PHP interpreter, powered by the Zend Engine, is free software released under the PHP License. PHP has been widely ported and can be deployed on most web servers on almost every operating system and platform, free of charge.

HTML

Hypertext Markup Language (HTML) is the standard markup language for creating we pages and web applications. With Cascading Style Sheets (CSS) and JavaScript it forms a triad of cornerstone technologies for the World Wide Web. Web browsers receive HTML documents from a webserver or from local storage and render them into multimedia web pages. HTML describes the structure of a web page semantically and originally included cues for the appearance of the document.

HTML elements are the building blocks of HTML pages. With HTML constructs, images and other objects, such as interactive forms, may be embedded into the rendered page. It provides a means to create structured documents by denoting structural semantics for text such as headings, paragraphs, lists, links, quotes and other items. HTML elements are delineated by tags, written using angle brackets. Tags such as <img /> and <input /> introduce content into the page directly. Others such as ... surround and provide information about document text and may include other tags as sub-elements. Browsers do not display the HTML tags, but use them to interpret the content of the page.

HTML can embed programs written in a scripting language such as JavaScript which affect the behavior and content of web pages. Inclusion of CSS defines the look and layout of content. The World Wide Web Consortium (W3C), maintainer of both the HTML and the CSS standards, has encouraged the use of CSS over explicit presentational HTML since 1997

Javascript

JavaScript (/ˈdʒɑːvəˌskrɪpt/), often abbreviated as JS, is a high-level, dynamic, weakly typed, object-based, multi-paradigm, and interpreted programming language. Alongside HTML and CSS, JavaScript is one of the three core technologies of World Wide Webcontent production. It is used to make webpages interactive and provide online programs, including video games. The majority of websites employ it, and all modern web browsers support it without the need for plug-ins by means of a built-in JavaScript engine. Each of the many JavaScript engines represent a different implementation of JavaScript, all based on the ECMAScript specification, with some engines not supporting the spec fully, and with many engines supporting additional features beyond ECM

As a multi-paradigm language, JavaScript supports event-driven, functional, and imperative (including object-oriented and prototype-based) programming styles. It has an API for working with text, arrays, dates, regular expressions, and basic manipulation of the DOM, but does not include any I/O, such as networking, storage, or graphics facilities, relying for these upon the host environment in which it is embedded.

Initially only implemented client-side in web browsers, JavaScript engines are now embedded in many other types of host software, including server-side in web servers and databases, and in non-web programs such as word processors and PDF software, and in runtime environments that make JavaScript available for writing mobile and desktop applications, including desktop widgets.

Although there are strong outward similarities between JavaScript and Java, including language name, syntax, and respective standard libraries, the two languages are distinct and differ greatly in design; JavaScript was influenced by programming languages such as Selfand Scheme.

CSS

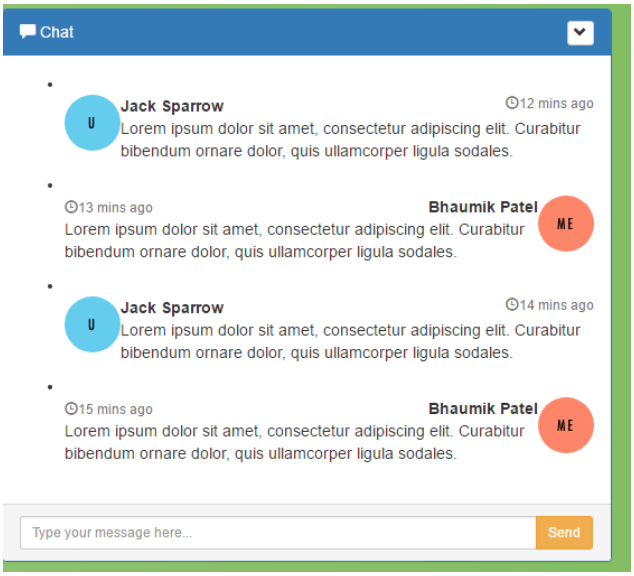
Cascading Style Sheets (CSS) is a style sheet language used for describing the presentation of a document written in a markup language. Although most often used to set the visual style of web pages and user interfaces written in HTML and XHTML, the language can be applied to any XML document, including plain XML, SVG and XUL, and is applicable to rendering in speech, or on other media. Along with HTML and JavaScript, CSS is a cornerstone technology used by most websites to create visually engaging webpages, user interfaces for web applications, and user interfaces for many mobile applications. CSS is designed primarily to enable the separation of presentation and content,

including aspects such as the layout, colors, and fonts. This separation can improve content accessibility, provide more flexibility and control in the specification of presentation characteristics, enable multiple HTML pages to share formatting by specifying the relevant CSS in a separate .css file, and reduce complexity and repetition in the structural content.

Separation of formatting and content makes it possible to present the same markup page in different styles for different rendering methods, such as on-screen, in print, by voice (via speech-based browser or screen reader), and on Braille-based tactile devices. It can also display the web page differently depending on the screen size or viewing device. Readers can also specify a different style sheet, such as a CSS file stored on their own computer, to override the one the author specified.

Changes to the graphic design of a document (or hundreds of documents) can be applied quickly and easily, by editing a few lines in the CSS file they use, rather than by changing markup in the documents.

The CSS specification describes a priority scheme to determine which style rules apply if more than one rule matches against a particular element. In this so-called *cascade*, priorities (or *weights*) are calculated and assigned to rules, so that the results are predictable.



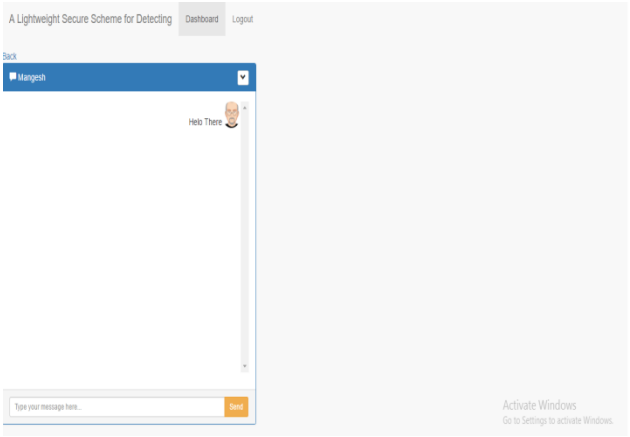


Fig:Chat Screen

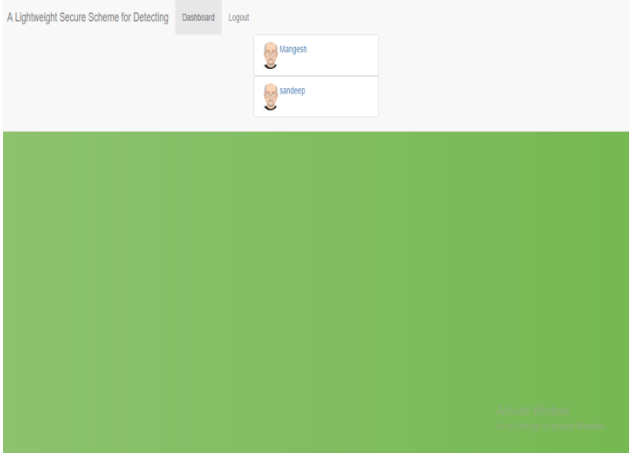
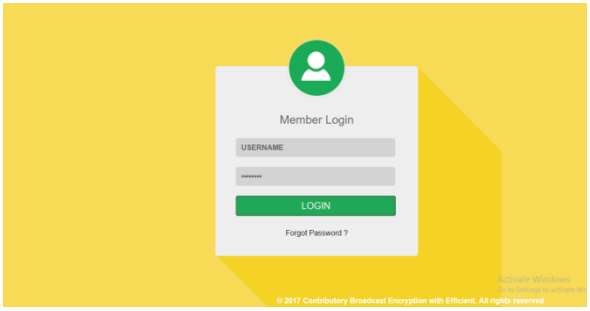


Fig:Dashboard Page

7. Result Analysis



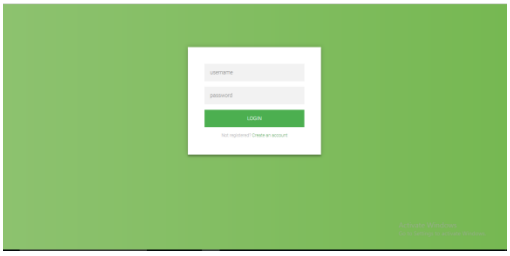


Fig: Login Page

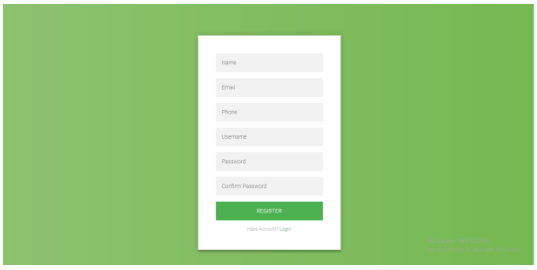


Fig: Registration Page

References

[1] Mishra, P. and Dutt, N., "Architectural description languages for programmable embedded systems", IEE Proceedings of Computers and Digital Techniques, May 2005, pp. 285–297

[2] Coelo Jr, C. J. N., Da Silva Jr., D. C., and Fernandes, A. O. "Hardware software codesign of embedded systems", Proceedings of the 11th Brazilian Symposium on Integrated Circuit Design, January 1998, pp. 2–8

[3] Ernst, R.: "Co design of embedded systems: status and trends", Proceedings of IEEE Design and Test, April–June 1998, pp.45–54

[4] "Run-Time Integration of Reconfigurable Video Processing Systems", Pete Sedcole, Peter Y. K. Cheung, George A. Constantinides, Wayne Luk , IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS, VOL. 15, NO. 9, SEPTEMBER 2007

[5] Nios II Hardware Development Tutorial, altera, December 2009Altera Corporation Website, www.altera.com, June 2006

[6] SELF-RECONFIGURABLE EMBEDDED SYSTEMS ON LOW-COST FPGAS, Ivan Gonzalez-George Washington University, Estanislao Aguayo-CIEMAT, Sergio Lopez-Buedo Universidad Autonoma de Madrid, 0272-1732/07/ G 2007 IEEE.