Digital Signature Manager

K.Gopalakrishnan[1]
Assistant Professor,
Nandha College of Technology ,
Erode.
Mail:gopalakrishnanbtech@gmail.com

S.Venkatesh[2],V.Naveen[3], S.TamilKumaran[4], R.Lakshmanan[5]
Nandha College of Technology [2,3,4,5] ,
Erode.
Mail:venkateshcse09@gmail.com[1]

Abstract—The contains options for managing the documents such as Bonafide certificate, gate pass, on-duty form and leave form for students with signatures of higher authorities (Head of the Department and Principal). From the student login, the requests are being filled by the students and send to top officials for authorization .From the Administrator login, the corresponding request forms are being examined and approved. The approved requests and corresponding forms are sending back to the students E-mail and it doesn't need any physical authorization because it is digitally signed and generated by the computer. The forms for various requests (Bonafide, Gate Pass, On Duty and Leave) and signature details of the HOD and Principal are converted from images to binary data and kept in databases so that the request forms are processed through the application itself. After that the student's requests are analyzed and examined by the administrator (HOD, Principal) then authorization that is signature is merged with the request form. Thus the application results in secure students requests processing with corresponding privileges for both top official and students. Various reports are generated dynamically by the administrative users for their further reference. Through this application, the concerns can process the information with better security.

I. Introduction

Digital signatures can be used for various types of documents where traditional pen and ink signatures were used in the past. However, the mere existence of a digital signature is not adequate assurance that a document is what it appears to be signature. The government and enterprise settings often need to impose additional constraints on their signature workflows such as restricting user choices and document behavior during and after signing. From the student login, the requests are being filled by the students and send to top officials for authorization .From the Administrator login, the corresponding request forms are being examined and approved. The approved requests and corresponding forms are sending back to the students E-mail and it doesn't need any physical authorization because it is digitally signed and generated by the computer. The forms for various requests (Bonafide, Gate Pass, On Duty and Leave) and signature details of the HOD and Principal are converted from images to binary data and kept in databases so that the request forms are processed through the application itself. When signing an document a person usually signs it in front of a notary public and other trusted authority after providing them satisfactory evidence of their identity. Because the notary is deemed trustworthy you can trust the signature the notary witnesses. Using a PKI is a method of providing a similar kind of trust.

II. LITRATURE SURVAY

Lightweight Privacy - Preserving Routing And Incentive Protocol**:** In this paper, proposed a privacy-preserving routing and incentive protocol, called PRIPO, for hybrid ad hoc wireless network. PRIPO uses micropayment to stimulate node cooperation without submitting payment receipts. The lightweight hashing and symmetric-key-cryptography operations are implemented to preserve the users' privacy. The nodes' pseudonyms are efficiently computed using hashing operations. Only a trusted party can link these pseudonyms to the real identities for charging and rewarding operations. Moreover, PRIPO protects the location privacy of the anonymous source and destination nodes. Extensive analysis and simulations demonstrate that PRIPO can secure the payment and preserve the users' privacy with acceptable overhead.

Node Cooperation in Hybrid Ad hoc Networks: A hybrid ad hoc network is a structure-based network that is extended using multi-hop communications. Indeed, in this kind of network, the existence of a communication link between the mobile station and the base station is not required: A mobile station that has no direct connection with a base station can use other mobile stations as relays. Compared with conventional (single-hop) structure-based networks, this new generation can lead to a better use of the available spectrum and to a reduction of infrastructure costs. However, these benefits would vanish if the mobile nodes did not properly cooperate and forward packets for other nodes. In this paper, we propose a charging and rewarding scheme to encourage the most fundamental operation, namely packet forwarding. We use "MAC layering" to reduce the space overhead in the packets and a stream cipher encryption mechanism to provide "implicit authentication" of the nodes involved in the communication. We analyze the robustness of our protocols against rational and malicious attacks. We show that - sing our solution collaboration is rational for selfish nodes. We also show that our protocols thwart rational attacks and detect malicious attacks.

Secure Incentive Protocol with Limited Use of Public-Key Cryptography: In multi-hop wireless networks, selfish nodes do not relay other nodes' packets and make use of the cooperative nodes to relay their packets, which has negative impact on the network fairness and performance. Incentive protocols use credits to stimulate the selfish nodes' cooperation, but the existing protocols usually rely on the heavy-weight public-key operations to secure the payment. In this paper, we propose secure cooperation incentive protocol that uses the public-key operations only for the first packet in a series and uses the light-weight hashing operations in the next packets, so that the overhead of the packet series converges to that of the hashing operations. Hash chains and keyed hash values are used to achieve payment non repudiation and thwart free riding attacks. Security analysis and performance evaluation demonstrate that the proposed protocol is secure and the overhead is incomparable to the publickey based incentive protocols because the efficient hashing operations dominate the nodes' operations. Moreover, the average packet overhead is less than that of the public-key based protocols with very high probability due to truncating the keyed hash values

Preserving Source - Location Privacy In Wireless Sensor Network Using Star Routing: In wireless sensor networks (WSNs), providing source-location privacy through secure routing is one of the most prosperous techniques. In this paper, we propose a routing technique to provide adequate source-location privacy with low energy consumption. We introduce this technique as the Sink Toroidal Region (STaR) routing. With this technique, the source node randomly selects an intermediate node within a designed STaR area located around the SINK node. The STaR area is large enough to make it unpractical for an adversary to monitor the entire region. Furthermore, this routing protocol ensures that the intermediate node is neither too close, nor too far from the SINK node in relations to the entire network. While ensuring sourcelocation privacy, our simulation results show that the proposed scheme is very efficient and can be used for practical applicationsWireless sensor networks can provide the world with a technology for real-time event monitoring for both military and civilian applications. One of the primary concerns that hinder the successful deployment of wireless sensor networks is source-location privacy. The privacy of the source location is vital and highly jeopardized by the usage of wireless communications. When traffic is transmitted wirelessly in the open air, any compatible receivers Within the transmission range of the sender is able to intercept the traffic. An adversary may be well-equipped with powerful transceivers to analyze the traffic patterns. They may be able to intercept traffic from one or multiple locations in network environment. Without an adequate protection of the routing paths, an adversary may be able to determine the source location by using RF localization techniques to trace back to the source in a hopby-hop approach. Therefore, even if a powerful encryption algorithm is used to protect the source identity, the adversary may still be able to determine the location of the source by monitoring the traffic patterns and routing paths.Privacy in a network consists of not only the privacy of the message content but also the privacy of the source and destination locations. The focus of this paper is on sourcelocation privacy. The confidentiality of the message content can be protected by encryption but the source location can be exposed in routing patterns. To be more concise, there may be different types of information besides the message content that are linked with a message transmission.In this paper, we propose a two-phase routing scheme that addresses the source-location privacy issue by using a unique routing process. In the routing process, the source node randomly determines an intermediate node from a pre-determined region around the SINK node. We call this region the Sink Toroidal Region (STaR). From the random intermediate node, the message will then be routed to the SINK node through the shortest path routing. The STaR routing method is performed for every message the source node sends to the SINK node in the network. We analyze the performance of the proposed STaR routing method and existing methods with network simulations. Our simulation results show that the STaR routing scheme can provide performance comparable to or better than the existing schemes while enhancing source-location privacy.

III. EXISTING SYSTEM

In the existing system, managing and authorizing the students request forms is processed manually. It causes loss of records may happen. And also the clarification and verification of those requested records takes lot of time and requires more manpower efforts. And also the students may misuse the requests and forms. Through this manual approach, cannot track all the students request details both approved and rejected in one place. The existing system has following disadvantages,

- The manual approach reduces the security aspects
- More time consuming for verifying and authorizing students requests
- Efficiency is less in authorizing the documents.
- Need more manpower effort.
- Less security and chances for misuse the authorized forms.

III. PROPOSED SYSTEM

The proposed system is managing documents through software in online environment. The higher officials can approve all the documents easily. The requests are being authorized digitally and it does not require any physical authentication. This method simplifies the security mechanism since every data is stored into the server database in a secured manner. This method is very helpful in various places where documents content are more confidential. The proposed system has following advantages,

- The proposed approach increases the security.

- Less time consuming in examine and analyze the student's requests.
- Efficiency is more and easier in authorizing the documents.
- Referencing the documents in future is simple and collectively since they are stored in database which can be accessed everywhere.
- Digitally approved requests no further manual approves needed.

IV. FEASIBILITY STUDY

The feasibility study deals with all the analysis that takes up in developing the project. Each structure has to be thought of in the developing of the project, as it has to serve the end user in a user-friendly manner. One must know the type of information to be gathered and the system analysis consist of collecting, Organizing and evaluating facts about a system and its environment. Three considerations involved in feasibility analysis are

- Economical Feasibility
- Operational Feasibility
- Technical Feasibility

V. EXPERIMENTAL ANALYSIS:

A. ADD DEPARTMENT

In this form the admin enter the department details such as department code, department name and name of HOD. Those details are stored in the department table that was created using SQL server

B. ADD STAFF

In this form admin entre the staff details such as staff id, staff name, address, department, contact number, email id and password. These details are used by the staff to login to the web site for requesting services.

C. ADD STUDENT

In this form admin entre the student details such as student id, student name, address, department, contact number, email id and password. These details are used by the student to login to the web site for requesting services.

D. APPROVE REQUEST

In this from staff gives reply to the student if he/she needs any information. After getting satisfied information from the student, the staff will proceed the request to appropriated person by approving the request.

E. APPLY NO DUE:

In this form student applies for the no due certificate by filling appropriate details which include student id, student name, address, department, year and reason for applying no due. This will be preceded to the appropriate staff for verification.

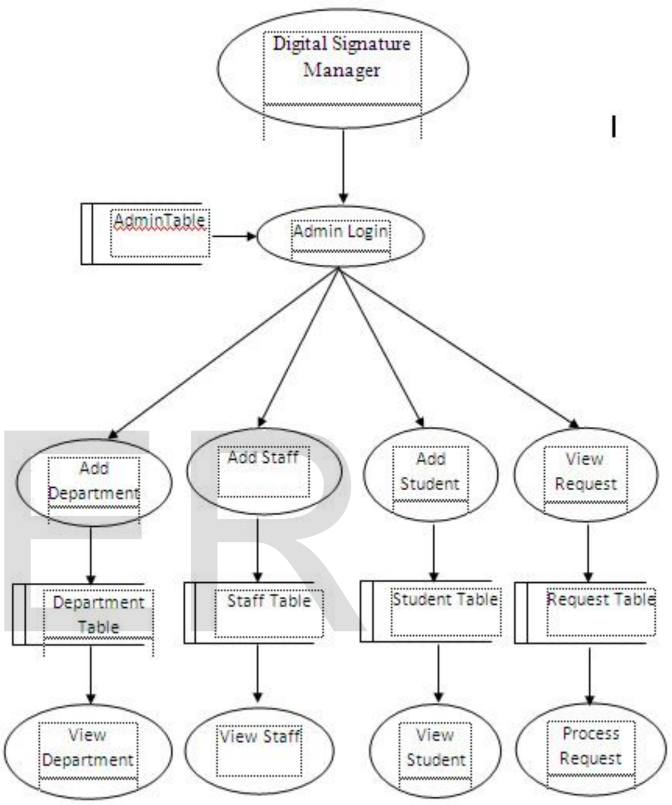
F. APPLY BONAFIDE:

In this form student applies for the bonafide certificate by filling appropriate details which include student id, student name, father's name, department, year and reason for applying bonafide. This will be preceded to the appropriate staff for verification.

G. VIEW STATUS:

In this form student view the status of the request that he/she had given to the staff by filling. After all the process had finished, the student will get a link for downloading the certificate from the website.

VI. DIAGRAMMATIC ANALYSIS:



V*I CONCLUSION AND FUTURE ENHANCEMENT*

Through this project, the activities of the College administration management process are carried out automatically without any physical records. This interface helps not only to administrator but also to students and staff for communication. This project includes the feature of applying Bonafide and No Due through online. After approved by appropriate authority the certificates will be generated automatically with HOD Signature. The feature of sending intimation to the student and staff via mail and SMS are added advantage.

Since the application is designed as web, any browser can be used to view the application. The change password helps to protect the accessibility of unauthorized persons. The application is tested well and end users satisfaction is found to be more. The application is designed such that minimum internet knowledge is required for end users to browse the web site.

REFERENCES

[1] M.MahmoudandX.Shen,‘‘FESCIM:Fair, Efficient, Secure Cooperation Incentive Mechanism for Hybrid Ad Hoc Networks,’’ IEEE Trans. Mobile Computer,vol.11,no.5, pp. 753-766, May 2012.

[2] M. Mahmoud and X. Shen, ‘‘Lightweight Privacy-Preserving Routing and Incentive Protocol for Hybrid Ad Hoc Wireless Networks,’’ in Proc. IEEE INFOCOM’11-Int’l Workshop Security Computers, Networking Comm. (SCNC), Shanghai, China, Apr. 2011, pp. 1006-1011.

[3] M. Mahmoud and X. Shen, ‘‘Anonymous and Authenticated Routing inMulti-Hop Cellular Networks,’’ in Proc. IEEE Int’l Conf. Comm. (IEEE ICC’09), Dresden, Germany, June 2009, pp. 839-844.

[4] N.Salem,L.Buttyan,J.Hubaux,andM.Jakobsson,‘‘Node Cooperation in Hybrid Ad-Hoc Networks,’’ IEEE Trans. onMobile Computing, vol. 5, no. 4, pp. 365-376, Apr. 2006.

[5] M.Mahmoud and X. Shen, ‘‘ESIP: Secure Incentive Protocol with Limited Use of Public-Key Cryptography forMulti-HopWireless Networks,’’ IEEE Trans. on Mobile Computing,vol.10,no.7, pp. 997-1010, July 2011.

[6] M.Mahmoud and X. Shen, ‘‘PIS: A Practical Incentive System for Multihop Wireless Networks,’’ IEEE Trans. on Vehicle Technology, vol. 59, no. 8, pp. 4012-4025, Oct. 2010.

[7] M. Mahmoud and X. Shen, ‘‘Stimulating Cooperation in Multi-Hop Wireless Networks Using Cheating Detection System,’’ in Proc. IEEE Conf. Information Comm. (IEEE INFOCOM’10),San Diego, CA, USA, Mar. 2010, pp. 776-784.

[8] S. Capkun, J.P. Hubaux, and M. Jakobsson, ‘‘Secure and Privacy-Preserving Communication in Hybrid Ad Hoc Networks,’’ EPFL-DI-ICA, Laussane, Switzerland, Tech. Rep. IC/2004/10, 2004.

[9] J. Kong, X. Hong, and M. Gerla, ‘‘An Identity-Free and On-Demand Routing Scheme Against Anonymity Threats in Mobile Ad Hoc Networks,’’ IEEE Trans. on Mobile Computing,vol.6, no. 8, pp. 888-902, Aug. 2007.

[10] A. Boukerche, K. El-Khatib, L. Korba, and L. Xu, ‘‘A Secure Distributed Anonymous Routing Protocol for Ad Hoc Wireless Networks,’’ J. Comput. Commun., vol. 28, no. 10, pp. 1193-1203, 2005.

[11] A.Suresh (2014), “Bespoke Image Search Engine Based On User Sensitivity”, International Journal on Recent and Innovation Trends in Computing and Communication, (IJRITCC) ISSN(Online): 2321-8169, ISSN(Print): 2652 – 2655, *Vol. 2, No.9, September 2014,* pp. 2652 – 2655.