ENHANCED ALERT PROTOCOL FOR MANET

Padmapriya.B,
Department of CSE,
SNS College of Technology,
Coimbatore
padmabalakrisnan@gmail.com

Madhuvandhi.B.R
Department of CSE,
SNS College of Technology,
Coimbatore
madhuvandhi45@gmail.com

Manikandan.K
Department of CSE,
SNS College of Technology,
Coimbatore
maniwhitejaguar@gmail.com

Chandruvignesh.C.
AP/Department of CSE
SNS College of Technology
Coimbatore
csechandru@gmail.com

Abstract - Mobile Ad Hoc Networks use anonymous routing protocols that hide node identities and/or routes from outside observers in order to provide anonymity protection. This is entitled as "Enhanced secured logging as a service using privacy preservation network in cloud architecture" is developed using ASP.Net as front end, SQL Server as the database and C# as coding language. Ajax 2.0 used as client server tool and scripting language as java script. Data and authorization security needed everywhere. In case dealing with huge number of data in a cloud server, secured logging is must. This is because cloud servers are easily accessible and any one can access anywhere at any time. So data should be preserved well for intruders, hackers and unauthorised user. In addition, as log data files often contain sensitive information, confidentiality and privacy of log records are equally important. Integrity of the log files and that of the logging process need to be ensured at all times

Keywords - Mobile ad hoc networks, anonymity, routing protocol, virtual proxy server.

I.INTRODUCTION

The main objective of this project is to develop a secured logging as a service in cloud architecture. So in the proposed method, privacy and preservation methods are enhanced. The secured logging contains six major functionalities to ensure more securities: Correctness, Confidentiality, and data logs, Privacy, Preservation and VPS (Virtual proxy server). The correctness deals with correctness data of the true history. Confidentiality deals with sensitive information not displaying during search. Data logs deals with the data history for identifying appropriate users. Privacy scheme deals with file linking and data access history. Preservation deals with enhanced colour code. And finally VPS deals with the proxy server for virtual data access. RAPID development of Mobile Ad Hoc Networks (MANETs) has stimulated numerous wireless applications that can be used in a wide number of areas such as commerce, emergency services, military, education, and entertainment.

ALERT: AN ANONYMOUS LOCATION-BASED EFFICIENT ROUTING PROTOCOL Networks and Attack Models and Assumptions ALERT can be applied to different network models with various node movement patterns such as random way point model and group mobility model. Consider a MANET deployed in a large field where geographic routing is used for node communication in order to reduce the communication latency. The location of a message's sender may be revealed by merely exposing the transmission direction. Therefore, an anonymous communication protocol that can provide intractability is needed to strictly ensure the anonymity of the sender when the sender communicates with the other side of the field.

Capabilities: By eavesdropping, the adversary nodes can analyze any routing protocol and obtain in- formation about the communication packets in their vicinity and positions of other nodes in the network. They can also monitor data transmission on the fly when a node is communicating with other nodes and record the historical communication of nodes. They can intrude on some specific vulnerable nodes to control their behaviour, e.g., with denial-of-service (DoS) attacks, which may cut the routing in existing anonymous geographic routing methods. In capabilities the attackers do not issue strong active attacks such as black hole. They can only perform intrusion to a proportion of all nodes. Their computing resources are not unlimited; thus, both symmetric and public/private key cannot be brutally decrypted within a reasonable time period. Therefore, encrypted data are secure to a certain degree when the key is not known to the attackers.

II.RELATED WORKS

We design, build, implement, and evaluate Cloud Proof, a secure and practical storage system specifically designed for the cloud setting. Our first novelty is the idea and the mechanism of enabling customers to prove to third parties when the cloud violates the IWF properties. This enabling of proofs is in addition to detecting the violations and is not present in previous work.

It includes the fact that the cloud can disprove false accusations made by clients; that is, in Cloud-Proof, clients cannot frame the cloud. We believe that such proofs are key to enabling security in SLAs with respect to these three properties. Customers and cloud can now establish a financial contract by which clients pay a certain sum of money for the level of security desired; customers have assurance that the cloud will pay back an agreed upon compensation in case their data security is forfeited because they can prove this violation. Without such proofs, the cloud can claim a smaller amount of damage to protect itself against significant financial loss and clients can falsely accuse the cloud. These proofs are based on attestations, which are signed messages that bind the clients to the requests they make and the cloud to a certain state of the data. For every request, clients and cloud exchange attestations. These attestations will be used in a lightweight auditing protocol to verify the cloud's behaviour

A. Future Enhancement

In future enhancement, the proxy server can be enhanced for more secured data transfer. Most of the time proxy refers to a layer-7 application on the OSI reference model. However, another way of proxying is through layer-3 and is known as NAT. The difference between these two technologies is the tier in which they operate, and the way of configuring the clients to use them as a proxy.

In client configuration of NAT, configuring the gateway is sufficient. However, for client configuration of a layer-7 proxy, the destination of the packets that the client generates must always be the proxy server (layer-7), and then the proxy server reads each packet and finds out the true destination. Because NAT operates at layer-3, it is less resource-intensive than the layer-7 proxy, but also less flexible. As we compare these two technologies, we might encounter a terminology known as 'transparent firewall'. Transparent firewall means that the layer-3 proxy uses the layer-7 proxy advantages without the knowledge of the client. The client presumes that the gateway is a NAT in layer-3, and it does not have any idea about the inside of the packet, but through this method the layer-3 packets are sent to the layer-7 proxy for investigation.

- Layer 7 virtual proxy servers can be used.
- Output can be shown using some medical domain for real time implementation.
- EC2 Cloud server can be implemented.
- Key character length can be increased for more security
- HTTPS can be implemented.
- NAT can be implemented

III.EXISTING SYSTEM

A. Secure Logging-as-a-Service

Security-as-a-service (SaaS) is an outsourcing model for security management. Typically, Security as a Service involves applications such as higher end data security services like Government Information, Military information, Banking Information and etc. These kinds of software delivered over the Internet but the term can also refer to security management provided in-house by an external organization.

Storing important data with cloud storage providers comes with serious security risks. The cloud can leak confidential data, modify the data, or return inconsistent data to different users. This may happen due to bugs, crashes, operator errors, or misconfigurations. Further-more, malicious security breaches can be much harder to detect or more damaging than accidental ones: external adversaries may penetrate the cloud storage provider, or employees of the service provider may commit an insider attack. These concerns have prevented security-conscious enterprises and consumers from using the cloud despite its benefits. These concerns are not merely academic. Amazon started receiving public reports that data on its popular Simple Storage Service (S3) had been corrupted due to an internal failure; files no longer matched customers' hashes. One day later, Amazon confirmed the failure, and cited a faulty load balancer that had corrupted single bytes in S3 responses intermittently, under load. Another example of data security violation in the cloud occurred when Google Docs had an access-control bug that allowed inadvertent sharing of documents with unauthorized readers. Even worse a cloud storage provider went out of business after losing 45% of client data because of administrator error.

Amazon's S3, Google's Big Table, HP, Microsoft's Azure, Nirvanix Cloud NAS, or others provide security guarantees in their Service Level Agreements (SLAs).

For example, S3's SLA and Azure's SLA only guarantee availability: if availability falls below 99:9%, clients are reimbursed a contractual sum of money. As cloud storage moves towards a commodity business, security will be a key way for providers to differentiate themselves. In this paper, we tackle the problem of designing a cloud storage system that makes it possible to detect violations of security properties, which in turn enables meaningful security SLAs.

The cloud security setting is different from the set-ting of previous secure storage or file systems research. The first difference is that there is a financial contract between clients and the cloud provider: clients pay for service in exchange for certain guarantees and the cloud is a liable entity. In most previous work, the server was some group of untrusted remote machines that could not guarantee any service. The second difference is that scalability is more important, as it is one of the primary promises of the cloud. Enterprises are important customers for the cloud; they have many employees requiring highly scalable access control and have large amounts of data.

IV.PROPOSED SYSTEM

Cloud computing security is an evolving sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing.

The method used here for security is keystroke logging. This allows only the right user to login at the right time. It is the action of tracking the keys struck on a keyboard, so that the person using the keyboard is unaware that their actions are being monitored. Whenever a user is created, the keystroke time of typing his/her password should be noted. When a user logins to sends details, the keystroke time for typing his/her password should matches with the time that is generated in the user creation. So this will provides a well security for the user's id and password from hackers.

A.Gaussian Mixture and Keystroke

Working with Gaussian Mixture and Keystroke:
The working of Gaussian Mixture and Keystroke based on the keyboard input given by the user
These values are calculated into 3 values, namely
Mean Value
Actual Value
Median Value
In case of the key stroke value said to be 3.76:
Mean value will be lesser than the actual value, the value will be 3.75 or 3.76
The actual values will the same value
The median will be increased from the actual value; the value will be 3.76 or 3.77.
Enabling high security can be done by the actual value only.

V. CONCLUSION

Previous anonymous routing protocols, relying on either hop-by-hop encryption or redundant traffic, generate high cost. Also, some protocols are unable to provide complete source, destination, and route anonymity protection. ALERT is distinguished by its low cost and anonymity protection for sources, destinations, and routes. It uses dynamic hierarchical zone partitions and random relay node selections to make it difficult for an intruder to detect the two endpoints and nodes en route. A packet in ALERT includes the source and destination zones rather than their positions to provide anonymity protection to the source and the destination. ALERT further strengthens the anonymity protection of source and destination by hiding the data initiator/receiver among a number of data initiators/ receivers. It has the "notify and go" mechanism for source anonymity, and uses local broadcasting for destination anonymity. In addition, ALERT has an efficient solution to counter intersection attacks. ALERT's ability to fight against timing attacks is also analyzed. Experiment results show that ALERT can offer high anonymity protection at a low cost when compared to other anonymity algorithms. It can also achieve comparable routing efficiency to the base-line GPSR algorithm.

ACKNOWLEDGEMENT

This research was supported in part by our project guide **Mr.C.Chandru Vignesh,** Assistant Professor, Department of Computer Science and Engineering for his exemplary guidance and valuable suggestions, which helped us in effectively developing our part.

REFERENCES

[1]. Bo Zhu, Zhiguo Wan, Mohan S. Kankanhalli, Feng Bao, Robert H. Deng, "Anonymous Secure Routing in Mobile Ad-Hoc Networks"

[2]. Haiying Shen, Member, IEEE, and Lianyu Zhao, Student Member, IEEE "ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs" , IEEE transactions on mobile computing, vol. 12, no. 6, June 2013

[3]. Karim El Defrawy, Member, IEEE, and Gene Tsudik, Senior Member, IEEE "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs" , IEEE transactions on mobile computing, vol. 10, no. 9, September 2011

[4]. Karim El Defrawy, Student Member, and Gene Tsudik, Senior Member, "PRISM: Privacy-friendly Routing In Suspicious MANETs (and VANETs)"

[5]. Xiaoxin Wu and Bharat Bhargava, Fellow, IEEE "AO2P: Ad Hoc On-Demand Position-Based Private Routing Protocol" , IEEE transactions on mobile computing, vol. 4,no. 4, july/august 2005

[6]. YIH-CHUN HUand ADRIAN PERRIG Carnegie Mellon University, USA "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks" , Wireless Networks 11, 21–38, 2005

[7] B. Zhu, Z. Wan, M.S. Kankanhalli, F. Bao, and R.H. Deng, "Anonymous Secure Routing in Mobile Ad-Hoc Networks," Proc. IEEE 29th Ann. Int'l Conf. Local Computer Networks (LCN), 2004.

[8] A.R. Beresford and F. Stajano, "Mix Zones: User Privacy in Location-Aware Services," Proc. IEEE Second Ann. Conf. Pervasive Computing and Comm. Workshops (PERCOMW), 2004.

[9] X. Wu, J. Liu, X. Hong, and E. Bertino, "Anonymous Geo- Forwarding in MANETs through Location Cloaking," IEEE Trans. Parallel and Distributed Systems, vol. 19, no. 10, pp. 1297-1309, Oct. 2008.

[10] K. El-Khatib, L. Korba, R. Song, and G. Yee, "Anonymous Secure Routing in Mobile Ad-Hoc Networks," Proc. Int'l Conf. Parallel Processing Workshops (ICPPW), 2003.

[11] S. Ratnasamy, B. Karp, S. Shenker, D. Estrin, R. Govindan, L. Yin, and F. Yu, "Data-Centric Storage in Sensornets with GHT, a Geographic Hash Table," Mobile Network Applications, vol. 8, no. 4, pp. 427-442, 2003.

[12] J. Raymond, "Traffic Analysis: Protocols, Attacks, Design Issues, and Open Problems," Proc. Int'l Workshop Designing Privacy Enhancing Technologies: Design Issues in Anonymity and Unobserva- bility (WDIAU), pp. 10-29, 2001.