Secure and Reliable Data Transaction Using Batch Verification In WSN

Munilakshmi M[1], Naveen Prasanth S[2], Nivedhitha V V[3], Vidhyalakshmi R[4]

[1, 2, 3] Dept of Computer Science and Engineering

[4]Assistant Professor, Dept of Computer Science and Engineering

[1, 2, 3, 4] Adhiyamaan College of Engineering, Hosur, India.

Abstract- *Wireless sensor network, is widely used for communication by transmitting data as packets from source to destination. However, when a single user wants to transmit a data to multiple receivers in emergency situation such as natural disasters, terrorist attacks, and sharing the current whereabouts to other users, such as notifying urgent business meeting information, these kind of data transactions need proper verification because there is a possibility that attacker will misuse this kind of data transaction. Hence proper authentication is needed for efficient data transaction. In our proposed work efficient authentication based secure data transaction is implemented. Initially, when data is transmitted from source to multiple destination, authenticated server (AS) will verify authentication of user and multiple receivers. From this process, unauthorized user can be identified and removed from the network.Outside attacker can be identified through secure authentication process and to secure our data from inside attackers' encryption MD5 is implemented. Hence it clearly shows that our proposed method achieves better solution and performance compared to existing available methods.*

Keywords- Authenticated server, Batch authentication, Data transaction, Security.

I. INTRODUCTION

When a data is sent from one MS to another, the information contained in the data is transmitted as plaintext. Data may also contain confidential information such as pin number and a link to a login page. Transmission of such confidential information as plaintext over an insecure network can be targeted by an adversary.This is surprising, as in our increasingly interconnected society, there are a number of situations where secure transmission of batch data can play a crucial role. In those applications, we should not compromise on security for the capability for batch dissemination of data.

To tackle the aforementioned problems, including security, efficiency, and scalability problems, we proposed an anonymous batch authentication and key agreement (ABAKA) scheme to build a secure environment for value-added services in VANETs. To avoid bottleneck problems, ABAKA is inspired by the concept of batch verification to simultaneously authenticate multiple requests sent from different vehicles using elliptic curve cryptography (ECC), which is adopted by the IEEE Trial-Use standard. Meanwhile, multiple session keys for different vehicles can also be negotiated at the same time. To the best of our knowledge, this is the first study that provides batch authenticated and key agreements for value added applications in VANETs.

II. LITERATURE REVIEW

All data transactions need a proper verification. Although WSNs have gained a lot of popularity, there are some serious limitations when implementing security imposed by resource limitations in memory, computing, battery life, and bandwidth. From one sensor node (source) data transmitted to base station (destination) through intermediate nodes. There are many routing algorithms designed for efficient data transaction among source and destination. To ensure reliable data delivery in group data transaction batch verification protocol is used. In our proposed work, to avoid unauthorized user data accessing, an authenticate server is implemented. In addition to this to enable secure data transaction light weight encryption algorithm is used. Hence our proposed work achieves better performance compared to existing methods.

III. EXISTING SYSTEM

Transmission of confidential information as plaintext over an insecure network can be targeted by an adversary (e.g., intercepting, reading and modifying the messages before it reaches the data center). The easy data and smart data are the only available protocols in the literature that enable secure transmission of data from one MS to another. however, no such protocol exists in the literature that can securely delivers the data to multiple recipients simultaneously. Verification of group of data transaction in secure and reliable way is not possible. For example, without an end-to-end (batch) message security mechanism in place, a malicious attacker could hijack and replace a batch message from the local authorities with one that will create social unrest. In addition, the protocol should be sufficiently lightweight, suitable for deployment on resource-constrained devices (e.g., limited battery)

IV. PROPOSED SYSTEM

To more efficiently handle multiple authentication requests, one solution is to perform a batch authentication for all incoming requests. Malicious user will generate fake request to create flooding attack and it will reduce performance of the system. To avoid this malicious a trusted authenticated server is implemented which verifies each user (both sender and multiple receivers in the network) authentication. Once the authentication is verified and acknowledgement has generated then the transaction will take place. However malicious users are identified there are different attackers available both inside and outside the network. To avoid this, in our work light weight encryption algorithm is used because most of the insider attacks were identified through AS and in order to protect our data from outside attacks encryption is implemented.

V. MODULES

A. IMPLEMENTATION OF WSN AND DATA GATHERING:

In this module, a WSN is implemented. The sensor nodes are randomly deployed in the network area. The BS node is deployed in the middle of the network for ease accessibility. All the sensor nodes produce data at periodic intervals and send the data to the BS frequently. A routing protocol is implemented to ensure the data transmission at the best path. Each transmission consumes different level of energy associated with it. The performance of the data collection is analyzed.

B. USER REGISTRATION MODULE:

In this module, both sender and receiver are considered to be user. Each and every user should register in our network for proper authentication process. This authentication reduces outside attackers by enabling efficient authenticating server as an in charge for it. Initially network is created and data transaction in done between single to multiple users authentication is done by AS. Once authentication process is completed then data transaction will take place.

C. BATCH VERIFICATION PROTOCOL:

The BVP protocol: a) provides mutual authentication between the sender MS and the Authentication Server, and between each recipient MS_i and the AS. b) maintains message confidentiality and integrity using AES with Counter (AES-CTR) and Message Authentication Code respectively, during messages transmission over an insecure network. c) allows the sending of only one of n-pieces of the secret code of the key by sender MS to each recipient MS. It has the following advantages: (i) sending a partial code to each recipient MS improves the overall security of the system, (ii) reduces the total communication overhead generated by the protocol. Each user’s original identity is kept secret during the authentication over the network. It protects the user against IMSI tracing and ID-theft attacks.

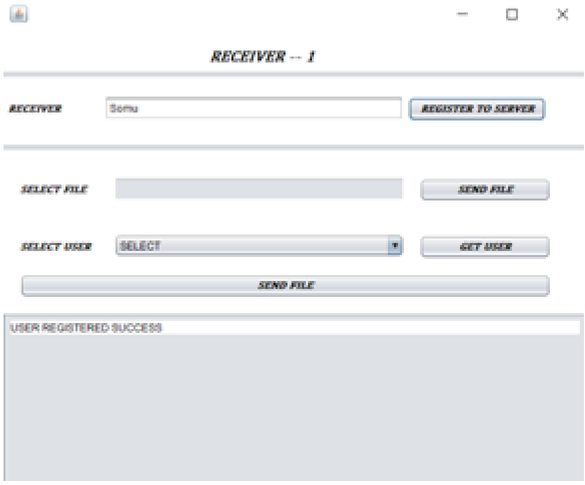
D. SECURE TRANSACTION:

In order to increase the security data transaction, MD5 algorithms can be used to hash the original passwords and the hash values, instead of the plaintext are stored in the database. During authentication, the input password is also hashed by MD5 in a similar way, and the result hash value is compared with the hash value in the database for that particular user. MD5 processes a variable-length message into a fixed-length output of 128 bits. MD5 works on blocks of 512-bits, and processes each block through 4 rounds, where each round in turn processes 16 sub-blocks (each 32-bits). The 512-bit message is divided into 16 sub-blocks before processing.

VI. CONCLUSION

Data transaction could be easily processed by utilizing networking. To secure our data during transaction several cryptographic algorithms were available. More number of research work has been concentrated on single packet transaction between source and destination. Focusing on batch data transaction, efficient approach should be needed and it was implemented in our work. To secure our data from both inside and outside attackers an efficient encryption and authentication scheme was deployed. Once data is transmitted both sender and receiver ID will be authenticated by AS which detect if any misbehaving node is included in the network. In addition to secure our data from inside attacker encryption algorithm has been implemented. Hence it clearly shows that our proposed method achieves better solution and performance compared to existing available methods.

VII. RESULTS

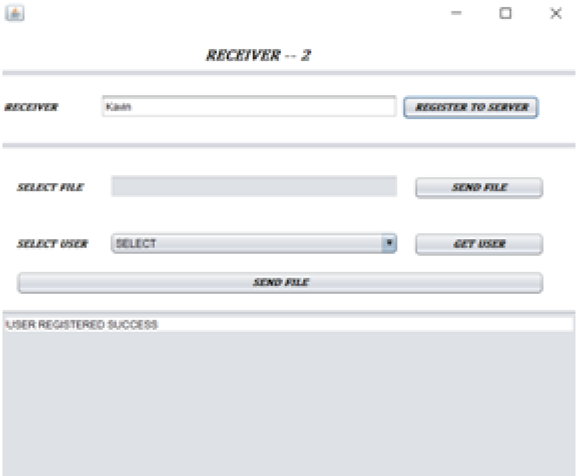


RECEIVER Somu

SELECT USER SELECT

USER REGISTERED SUCCESS

Fig.1. Receiver-1 is registered

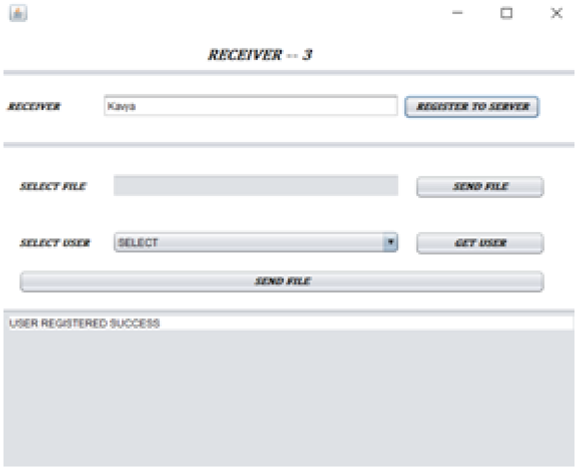


RECEIVER Kavin

SELECT USER SELECT

USER REGISTERED SUCCESS

Fig.2. Receiver-2 is registered

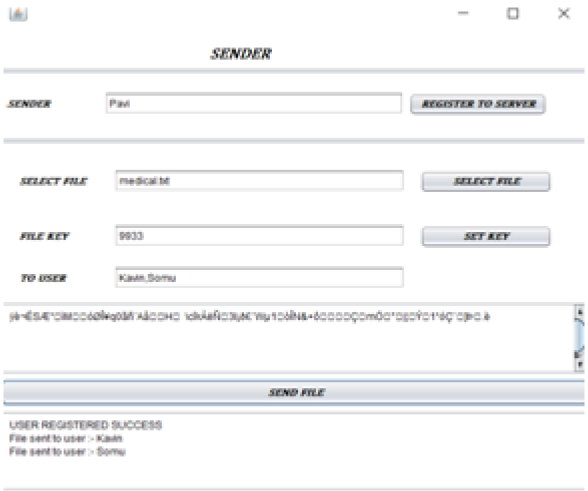


RECEIVER Kavya

SELECT USER SELECT

USER REGISTERED SUCCESS

Fig.3. Receiver-3 is registered



SENDER Pavi

SELECT FILE medical.txt

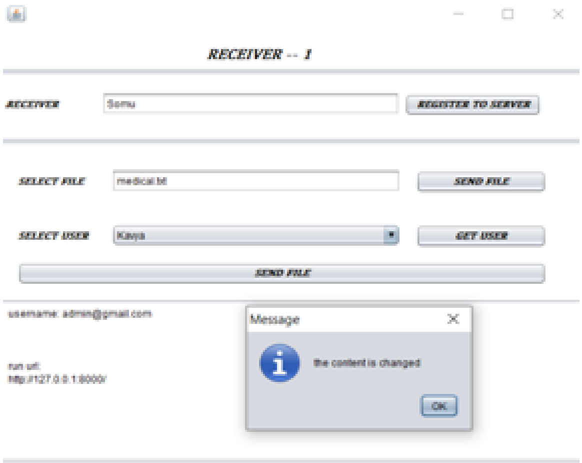
FILE KEY 9933

TO USER Kavin,Somu

[illegible]

USER REGISTERED SUCCESS
File sent to user :- Kavin
File sent to user :- Somu

Fig.4. Sender is registered and file is sent



RECEIVER Somu

SELECT FILE medical.txt

SELECT USER Kavya

username: admin@gmail.com

run url:
http://127.0.0.1:8000/

Message

the content is changed

Fig.5. File is received

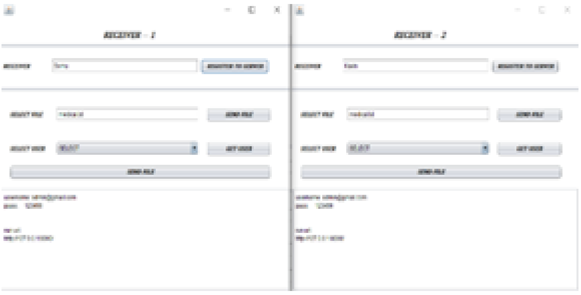


Fig.6. If the content is modified the file cannot be sent

REFERENCES

[1] P. Mondal and P. Desai, “An efficient SMS-based framework for public health surveillance,” in Proc. IEEE PCHT, 2013, pp. 244-247.

[2] B. DeRenzi, “Improving community health worker performance through automated SMS,” in Proc. 5th ICDT, 2012, pp. 25-34.

[3] J. Chen, L. Subramanian, and E. Brewer, “SMS-based web search for low-end mobile devices,” in Proc. MobiCom, 2010, pp. 125-135.

[4] A. Castiglione, G. Cattaneo, A. Santis, and U. F. Petrillo, “SPEECH: secure personal end-to-end communication with handheld,” in Proc. ISSE - Securing Electronic Busines Processes, 2006, pp. 287-297.

[5] J. Lee and Y. Oh, “A study on providing the reliable and secure SMS authentication service,” in Proc. IEEE Intl Conf on Ubiquitous Intelligence and Computing, Bali, 2014, pp. 620-624.

[6] P. Gope and T. Hwang, “Lightweight and energy-efficient mutual authentication and key agreement scheme with user anonymity for secure communication in global mobility networks,” IEEE System Journal, Mar. 2015, accepted.

[7] P. Traynor, W. Enck, and P. McDaniel, “Mitigating attacks on open functionality in SMS-capable cellular networks,” IEEE/ACM Transactions on Networking, vol. 17, no. 1, pp. 40-53, 2009.

[8] N. Saxena and N. S. Chaudhari, “EasySMS: a protocol for end-toend secure transmission of SMS,” IEEE Transactions on Information Forensics and Security, vol. 9, no. 7, pp. 1157-1168, Jul. 2014.

[9] P. Vijayakumara, S. M. Ganesha, L. Deboraha, and B. Rawalb, “A new SmartSMS protocol for secure SMS communication in m-health environment,” Computers & Electrical Engineering, pp. 1-17, 2016.

[10] Y. Yang , J. Lu, K.-K. R. Choo, and J. K. Liu, “On lightweight security enforcement in cyber-physical systems,” Lightweight Cryptography for Security and Privacy, LNCS vol. 9542, pp. 97-112, Jan. 2016. [Online]. http://dx.doi.org/10.1007/978-3-319-29078-2 6.

[11] C. Zhang, X. Lin, R. Lu, P. Ho, and X. Shen, “An efficient message authentication scheme for vehicular communications,” IEEE Trans. on Vehicular Technology, vol. 57, no. 6, pp. 3357-3368, 2008.

[12] J. L. Huang, L. Y. Yeh, and H. Y. Chien, “ABAKA: an anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks,” IEEE Transactions on Vehicular Technology, vol. 60, no. 1, pp. 248-262, 2011.

[13] S. J. Horng, S. F. Tzeng, Y. Pan, P. Fan, X. Wang, T. Li, and M. K. Khan, “b-SPECS+: batch verification for secure pseudonymous authentication in VANET,” IEEE Transactions on Information Forensics and Security, vol. 8, no. 11, pp. 1860-1875, Nov. 2013.

[14] T.W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, “SPECS: secure and privacy enhancing communications schemes for VANETs,” Ad Hoc Networks, vol. 9, pp. 189-203, 2011.

[15] N. Saxena and N. S. Chaudhari, “Secure encryption with digital signature approach for short message service,” in World Congress on WICT.

[16] Y. Zhou, X. Zhu, and Y. Fang, “MABS: multicast authentication based on batch signature,” IEEE Transaction on Mobile Computing, vol. 9, no. 7, pp. 982-993, Jul. 2010.