Indian Journal of Science and Technology, Vol 9(21), DOI: 10.17485/ijst/2016/v9i21/87066, June 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Authentication Framework for Military Applications Employing Wireless Sensor Networks and Private Cloud

S. Magesh*, K. Nimala and A. R. Nagoor Meeran

Department of Information Technology, SRM University, Chennai - 603203, Tamil Nadu, India;
magesh.sriramalu@gmail.com, nimskt@gmail.com, nagoormeeran.a@ktr.srmuniv.ac.in

Abstract

Objectives: To provide an authentication framework between military data centres pertaining to different levels of operations within the private cloud and a simple authentication schema for authenticating users at the wing-commander level in the special sinks deployed in our territory closer to line of control. **Methods:** In order to achieve the above mentioned objectives, we designed a conceptual defense structure that will highlight the various hierarchical levels of military operations. Military WSNs and data centres will utilize the designed simple authentication schema to improve the lifetime of the WSNs. The methodology adopted primarily consists of modifications to the existing Kerberos setup, so that it could fit the conceptual defense structure by utilizing Heimdal Kerberos distribution. Heimdal's modified Kerberos distribution is utilized in the cloud gateway system to create Kerberos Distribution Center. The modified Kerberos equations are provided in this paper. **Findings:** Based on the simulations carried out, it is identified that number of messages required for various dialogs for modified Kerberos is relatively less compared to the original version of Kerberos. The response time for modified Kerberos in single realm and cross realm based on different number of requests showed that modified Kerberos is performing better and efficient with respect to the response time metric. Minimum number of messages required for Kerberos Authentication using v4 (Simple dialog), v4 (Secure dialog), v4 (Authentication dialog), v5 (Request for service in another realm using Inter realm authentication) are 3, 5, 6 and 7 respectively. Response times range for single realm lie in the range of 3ms to 20ms approximately for 10 to 100 requests per minute. Response times range for cross realm lie in the range of 7ms to 47ms approximately for 10 to 100 requests per minute. The authentication time to authenticate instructions received at special sinks from level 1 resource via cloud gateway ranges from 4.5ms to 6ms for message sizes ranging from 100 bytes to 1000 bytes. The response times obtained from single realm authentication indicates lesser values as compared against cross realm authentication which is in consensus with the theory of Kerberos. **Applications:** The proposed scheme finds its application in all mission critical tasks where the time taken for successful authentication of users should be drastically reduced to improve the system performance.

Keywords: Authentication, Cloud, Defense, Kerberos, Wireless Sensor Networks

1. Introduction

Since sensitive data transactions are a characteristic of defense operations, it is more apt to provide different sets of services for defense through private cloud and not through a public cloud. To increase the scope of operation of defese cloud, it is feasible and easy to integrate WSNs for military applications with private defense cloud. Sensor Event as a Service (SEaaS) and Sensing as a Service (SaaS) through adaptor abstraction can be provided to the various data centres of defense through private cloud[1]. Much previous research work on improving military operations focussed on enhancing the power of operation of WSNs at the battlefield. In this paper, we focus at integrating the military WSNs along with private defense cloud. This paper also proposes an authentication frame-

*Author for correspondence

work between various levels of military data centres and between military data centre and special sinks of WSNs deployed in the battle field. A simplified user and message authentication scheme with a single transmission between military data centre and special sink through cloud gateway is also proposed. Communication between military WSNs and private defence cloud shall happen in a secured manner and is a two way process. Special sinks present in the military WSN transmit and receive information and instructions respectively to and from the data centre present at the wing-commander level. Based on the instructions received at the special sinks, necessary warfare actions shall be initiated at the battle field. Category 2 nodes and category 3 nodes are considered to be special mobile cloud computing nodes that shall be assembled from specially designed hardware (measuring about 2 feet by 2 feet by 2 feet). These nodes are connected to the data centres through IP based network with the features of 3G wireless security[2].

Grid computing and cloud computing are so similar that grid security technique can be applied to cloud computing[3]. The current Grid Security Infrastructure (GSI) technique has poor scalability[4]. SSL Authentication Protocol (SAP)[5] along with X.509 certificate based Public Key Infrastructure (PKI) authentication framework, when applied to cloud computing is less efficient[6]. Identity based authentication for cloud computing[3], based on the identity based hierarchical model for cloud computing claimed that the authentication model was light weight than SAP and is useful for outsourcing computational tasks to powerful servers.

Open standards are utilized to deliver an independent, policy based cloud authentication platform, supporting the integration of various authentication methods[7].

Authentication framework[8] in the cloud and its application to mobile users based on[6] results in a new authentication paradigm for users of mobile technologies over the cloud.

Various use case scenarios[9] are provided for delivering Kerberos authentication as a service over the cloud. This article provides only background assumptions and requirements for porting Kerberos authentication as a service over the cloud. Based on the extensive survey of literature work, it is noted that only this article provides a use case scenario for Kerberos authentication service over private cloud. But, it lacks modelling and simulation results of Kerberos authentication as a cloud service.

Communication security operations is utilized in the military, primarily the cryptographic and transmission security portions[10]. Communications security operations are protective measures taken to deny unauthorized persons, telecommunications information.

The transition of Department of Defense (DoD)[11] is stated in the perspective of authentication using a combination of three pillars of authentication namely "something you know, something you have or something you are". A new multi tier adaptive military MANET security protocol[12] is proposed using hybrid cryptography and sign cryption. It also deals with securing military MANET communication from the perspectives of cryptographic methods used in MANETs, hybrid key management protocols and structural organization of the military MANETs.

The importance of secure, integrated and efficient networking in Digital Battle Fields (DBFs)[13], is expressed which comprises of various critical networking components. Two tiered Unmanned Aerial Vehicle –Mobile Backbone Networks (UAV-MBN)[14,15] have been proposed for DBFs utilizing the heterogeneous structure of military MANETs, which significantly facilitates key management for secure communication. PLA[16] resembles the verification procedures used to check the authenticity of money. Eight requirements of strong authentication[17] is identified in a military MANET for tactical scenario. The various requirements for authentication in tactical MANETs include Strong authentication, Easy to Use, Scalable, Low Latency, Low Control Overhead, Support Re-authentication, Support Revocation, Interoperable. Provably secure multi factor authentication for cloud computing systems is discussed based on SecAuthn[18]. Multi clouds concept is used to perform authentication scheme using Integrated User Authentication Method and Brokerage authentication center[19]. PB verification and authentication for server[20] using multi communication is used in cloud environments. Multi factor user authentication based group communication is utilized for cloud technology[21].

2. Authentication Framework and Schema

For the system organization presented in Section 2 of this paper, communications happen only in a hierarchical

manner with security procedures implemented in a stringent and strategic manner.

Within private defence cloud, there are various levels of data centres. We attribute the data centre at top level to brigadiers (Level 3). Data centre at the middle level (Level 2) is used only by officer generals, whereas data centre at the bottom level (Level 1) is used by Wing Commanders. It is possible for data centre systems at level 3 to communicate only with data centre systems at level 2. Data centre systems at level 2 can communicate with data centre at both level 3 and level 1. Data Centre systems at level 1 shall communicate with special sinks via cloud gateway and data centre systems at level 2.

To authenticate data centre systems among themselves at different levels, we employ Kerberos authentication mechanism.

We propose an authentication scheme to authenticate instructions received at special sinks from level 1 resource via cloud gateway.

The authentication schema used is specially designed to increase the energy efficiency of the special sink and also reduce the time taken to perform actions based on the message received from level 1 resource while still maintaining security.

2.1 Authentication Schema: H(Msg) || E(Msg) || H(Pswd)

H(Msg) - Hashed Message
E(Msg) - Encrypted Message
H(Pswd)- Hashed Password

The username and corresponding password for every user at level 1 will also be stored in the special sinks via Over the Air (OTA) programming techniques followed in Wireless Sensor Networks[22]. When a message or instruction needs to be transmitted to the regiments from the data centre, the message is encrypted and also the hash value of the message is calculated. The encrypted message, hashed message and hashed password are concatenated with each other. The concatenated message is sent to the special sink in the war zone. The special sink de-concatenates the message, to extract the concatenated three components. Once the password is verified and the integrity of the message is checked, the message is transmitted by the special sink to all the regiments for necessary actions.

We have also modified Kerberos version 5, secure authentication dialogue equations to suit our framework and simulated using Heimdal Kerberos Version[23] and Cloud Analyst. The equations provided below utilize the entities such as Cluster Head (CH), GateWay Kerberos Server, GateWay Functional Server (GWFS), Source Personnel (SP), Destination Personnel (DP).

CH→GWKS : Options||ID_{CH}||$Realm_{CH}$||ID_{GWKS}||Times||Nonce1

GWKS→CH : $Realm_{CH}$||ID_{CH}||$Ticket_{GWFS}$||$E(K_{CH,GWKS}$, [$K_{CH,GWFS}$||Times||Nonce1||$Realm_{GWFS}$||ID_{GWFS}])||$E(K_{CH}$[$K_{CH,GWKS}$])

$Ticket_{GWFS}$=$E(K_{GWFS}$[Flags||$K_{CH,GWFS}$||$Realm_{CH}$||ID_{CH}||AD_{CH}||Times])

a. Exchanges between CH and GWKS to Obtain Ticket $_{GWFS}$

CH→GWFS : Options|| $Ticket_{GWFS}$||$Authenticator_{CH}$

$Authenticator_{CH}$=$E(K_{CH,GWFS}$,[ID_{CH}||$Realm_{CH}$||TS_1])

GWFS→CH : $E(K_{CH,GWFS}$[TS_2|| Subkey|| seq#])

Cluster Head/Gateway Functional Server Authentication Exchange to obtain service

SP→GWKS : Options||ID_{SP}||$Realm_{SP}$||ID_{GWKS}||Times||Nonce1

GWKS→SP : $Realm_{SP}$||ID_{SP}||$Ticket_{DP}$||$E(K_{SP,GWKS}$,[$K_{SP,DP}$||Times||Nonce1||$Realm_{DP}$||ID_{DP}])||$E(K_{SP}$[$K_{SP,GWKS}$])

$Ticket_{DP}$=$E(K_{DP}$[Flags||$K_{SP,DP}$||$Realm_{SP}$||ID_{SP}||AD_{SP}||Times])

b. Exchanges between SP and GWKS to Obtain Ticket $_{DP}$

SP→DP : Options|| $Ticket_{DP}$||$Authenticator_{SP}$

$Authenticator_{SP}$=$E(K_{SP,DP}$,[ID_{SP}||$Realm_{SP}$||TS_1])

DP→SP : $E(K_{SP,DP}$[TS_2|| Subkey|| seq#])

c. SP/DP Authentication Exchange to Obtain Service

3. Simulation Scenario and Results

The private cloud presented in Section 2 is simulated using CloudAnalyst. The CloudAnalyst is built directly on top of CloudSim framework leveraging the features of the original framework[24]. CloudSim is a comprehensive platform which is used to model data centers, service

brokers, scheduling and allocation policies of a large scale cloud platform. Various features of CloudAnalyst such as ease of use, ability to define a simulation with high degree of configurability and flexibility, graphical output, repeatability, ease of extension, made us to utilize the same in our simulation. The messages to and from the special sinks of WSN is transmitted to the cloud application service broker (Cloud gateway). Cloud application service broker in cloudAnalyst is analogous to cloud gateway in the system described in this paper.

The various configuration parameters used in the CloudAnalyst to simulate a private defence cloud with military Wireless Sensor Network are:

- Node base within a single time zone (since the nodes are deployed in the warzone)
- Special sinks in military WSN are considered analogous to the users who receive responses and transmit event information periodically to the data centre via cloud application service broker. The number of users (special sinks) are configured to be 50/sq.km.
- Every message from every special sink to the cloud application service broker is configured as a single cloudlet.
- The following table (Table 1.) shows the simulation details of data centre and corresponding virtual machines in CloudAnalyst.

The message from different machines inside the data centre intended for regiments is sent to the special sinks via cloud application service broker. The message is encrypted using AES (Advanced Encryption Standard) and hashing algorithm employed is MD5.

The concatenation process in the authentication framework, the reverse of concatenation, authentication, encryption and decryption were performed using Java since it supports multi threaded environment as required by a distributed environment such as cloud platform and WSN. This Java program is loaded and executed at the special sink. We computed the time taken to authenticate a message and also carried the same for various message sizes using a Java program. The following graph shows the behaviour of our authentication schema with respect to different message sizes.

The x-axis of the above graph (Figure 1.) consists of size of message in bytes and the y-axis of the graph consists of authentication time in milliseconds.

Table 1. Configuration details used in CloudAnalyst simulation

Configuration Parameter	Value Used in the Simulation
Virtual Machine Memory	1024Mb
Data Centre Architecture	X86
Data Centre OS	Linux
Data Centre Virtual Machine Monitor	XEN
No.of machines in the data centre	20
Memory per machine in the data centre	2048Mb
No. of processors per machine in the data centre	4

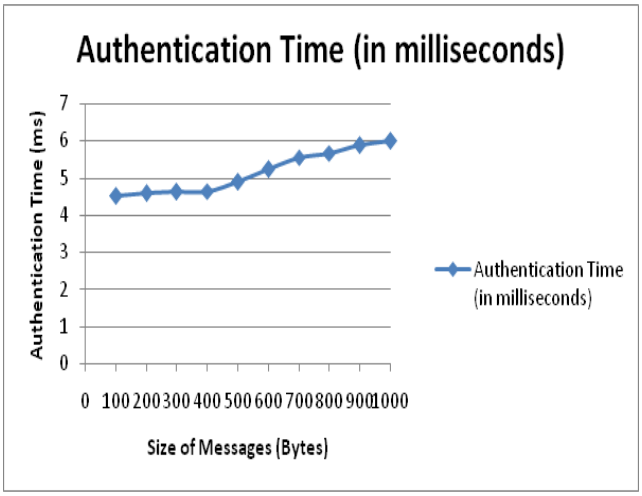

Figure 1. Authentication time for different message sizes.

The proposed authentication scheme combined the services of data confidentiality, user authentication and data integrity in a single message transmission as against Kerberos authentication mechanism. Table 2 provides the minimum number of messages required to authenticate a user using different Kerberos versions.

For Kerberos authentication, we utilized CloudAnalyst, a simulator for cloud computing to create virtual machines within two data centers with Ubuntu distribution of Linux. These client systems are configured to issue 10 to 15 requests per minute. Kerberos distribution component in client timestamps the transaction, that ultimately authenticates it to the application servers.

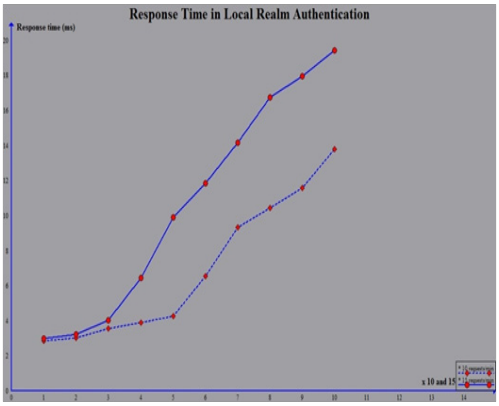

Figure 2. Response time with single realm.

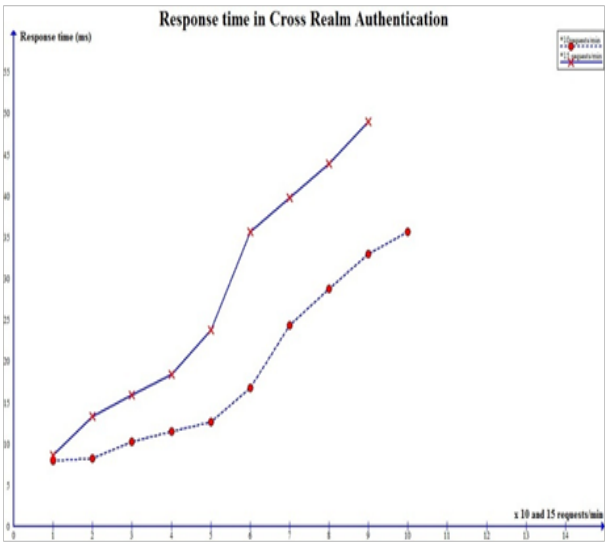

Figure 3. Response time with cross realm using one hop server.

Heimdal Kerberos server distribution is used in the cloud gateway system created in the CloudAnalyst to implement Kerberos Distribution Center (KDC).

The following graphs (Figure 2 and Figure 3) provide results for response time based on local realm authentication and cross-realm authentication respectively.

4. Conclusion

In this paper, we defined a system organization that provided the detailed architecture of private defense cloud and its integration with military WSN for efficient operations. We also proposed an authentication framework between different levels of data centers in the defense department and an authentication schema which is efficient in terms of number of communications required to provide services such as user authentication, message authentication and data confidentiality. We simulated the described system organization using CloudAnalyst and the authentication schema using multi threaded Java code. We also showed the behavior of our authentication schema with respect to different message sizes based on authentication time.

Table 2. Information on Kerberos authentication

Different Dialogs in Kerberos	Minimum No. of Messages Required
Version 4 - Simple Dialog	3
Version 4 - More Secure dialog	5
Version 4 - Authentication dialog	6
Version 5 - Request for service in another realm using Inter realm Authentication	7

5. References

1. Reddy AMV, Katru SP, Padmanabh K. Can we plug wireless sensor network to cloud. SETLabs Briefings; 2009.
2. NetworkWorld. Available from: www.networkworld.com/.../092310-cloud-computing-afghanistan.html
3. Li H, Dai Y, Tian L, Yang H. Identity based authentication for cloud computing, cloud computing. Springer-Verlag: Berlin Heidelberg; 2009. p. 157–66.
4. Foster I, Kesselman C, Tsudik G, Tuecke S. A security architecture for computational grids. Proceeding of the 5thACM conference on communications and security; 1998. p. 83–92.
5. Freier AO, Kocher PC. The SSL protocol, v3.0. Internet-Draft; 1996. p. 1–63.
6. Mao W. An identity based non interactive authentication framework for computational grids. HP Labs: UK; 2004.
7. Song Z, Molina J, Lee S, Lee H, Kotani S, Masuoka R. TrustCube: An infrastructure that builds trust in client. Future of Trust in Computing; 2009. p. 68–79.
8. Song Z, Molina J, Lee S, Lee H, Kotani S, Masuoka R, Shi E. Authentication in the clouds: A framework and its application to mobile users. CCSW; 2010. p. 1–6.
9. Use case scenarios for kerberos provided by MIT. Available from: https://www.oasis-open.org/committees/.../Kerberos-Cloud-use-cases-11june2010.pdf
10. Field Manual 24-12. Communications in a come as-you-are war. USA: Department of the Army; 1990.
11. Liebig J. Authentication on DoD information systems. GSLC Practical Assignment, Version 1.0; 2004.

12. Yavuz AA, Alagoz F, Anarim E. A new multi tier adaptive military MANET security protocol using hybrid cryptography and signcryption. Turkish Journal of Electrical Engineering and Computer Science. 2010; 18(1):1–21.
13. The Warfighter Information network- Tactical (WIN-T). Available from: http://www.globalsecurity.org/military/systems/ground/win-t.htm
14. Gu DL, Pei G, Ly H, Gerla M, Hong X. Hierarchical routing for multi layer ad-hoc wireless networks with UAVs. IEEE MILCOM 2000; 2000. p. 310–14.
15. Kong J, Luo H, Xu K, Gu DL, Gerla M, Lu S. Adaptive security for multi layer ad-hoc networks. Special Issue of Wireless Communications and Mobile Computing. 2002; 2:533–47.
16. Candolin C, Lundber J, Kari H. Packet level authentication in military networks. Finland: Helsinki University; 2005. p. 1–3.
17. Tang H, Salmanian M, Chang C. Strong authentication for tactical mobile ad-hoc networks. Canada: Technical Memorandum; 2007.
18. Nagaraju S, Parthiban L. SecAuthn: Provably secure multi-factor authentication for the cloud computing system systems. Indian Journal of Science and Technology. 2016; 9(9):1–18.
19. Choi J-H, Lee S-H, Kim M-K. Integrated user authentication method using BAC (Brokerage Authentication Center) in multi-clouds. Indian Journal of Science and Technology. 2015; 8(25):1–7.
20. Kumar DG, Rajasekaran S, Prabu R. PB verification and authentication for server using multi communication. Indian Journal of Science and Technology. 2016; 9(5):1–6.
21. Hong S. Multi-factor user authentication on group communication. Indian Journal of Science and Technology. 2015; 8(15):1–6.
22. Hagedorn A, Starobinski D, Trachtenberg A. Rateless Deluge: Over-the-air programming of wireless sensor networks using random linear codes. Proceedings of International Conference on Information Processing in Sensor Networks, IPSN'08; St Louis, MO. *2008. p. 457–66.*
23. Heimdal kerberos distribution. Available from: www.h5l.org
24. Wickremasinghe B, Calheiros RN, Buyya R. CloudAnalyst: A cloudSim-based modeller for analyzing cloud computing environments and application, 24th IEEE International Conference on Advanced Information Networking and Applications; Perth, WA. 2010. p. 446–52.