International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-4 Issue-3, February 2015

A New Multi- Authentication Scheme using Attribute Aggregation

Faris M. Al-Athari, Abdulameer K. Hussain

Abstract— ***This paper presents an authentication method for ensuring the best user's identity proof. The authentication procedure depends on identifying different user's attributes since no single person or system knows anyone's complete set of identity attributes. Individuals are most likely to know the majority of the attributes that serve to identify them. In this scheme, different attributes are defined to serve two purposes. First, to authenticate each user depending on weights assigned to each attribute of the authenticated users and these are subjected to different statistical measurements. Second, depending on the result of this statistical measurement, the system grants users different privileges using access control mechanism and thus we construct a multi-level authentication. Finally, the system applies a combination of different attributes which differs from other traditional attribute authentication.***

Index Terms— ***Attribute-based systems, Authentication, Privilege, Identity Providers.***

I. INTRODUCTION

The most strong scheme for providing a highly granular, scalable and semantically rich method for access control and authorization is Attribute-based system [1]. This type of schemes has a service provider (SP) which defines policies that dictate the set of attributes required for accessing its services. Different levels of access can be provided based on what attribute values the user possesses. So, this scheme is especially suitable for distributed systems, where maintaining real time synchronization among access control lists is a huge problem [2]. Attribute-based systems have many advantages compared to traditional systems like role based access control [1], but these schemes have some practical constraints. First of these limitations, it is very difficult for a service provider to directly verify each user's attributes in real time. Traditionally, the problem of verification is addressed by requiring users to get their attributes bundled into credentials, verified and digitally signed by an Identity Provider (IdP) [3],[4]. These credentials are trusted by the SP (which acts as a relying party). We argue that this approach limits the attribute set that can be used because IdPs might not be willing to certify certain attributes or it might not be efficient for them to verify these attributes. For example, the IdPs may be unwilling to certify attributes that are not identity related. Another problem is with rapidly changing attributes or addition of new attributes. Fresh credentials need to be issued by the IdP every time an attribute value changes or a new attribute is added. The second limitation is that these schemes require that all relying parties have reliable access to all the IdPs' public keys [5]. This scheme can either have only a few IdPs effectively overloading them and making them lucrative targets for attacks or have a high number of IdPs, making it difficult for each relying party (RP) to know every IdP's public key reliably [5],[6]. We argue that this represents a performance bottleneck in current systems. The third constraint is that, in current systems, only a few user attributes are available. In order to achieve a high granularity in attribute-based systems, a large number of attributes are desired. Since an attribute is any parameter that characterizes a user, a single IdP may not be able to verify every attribute and issue credentials. If there are multiple IdPs, the user may be required to aggregate these attributes before presenting them to the SP [7], [8]. The final limitation is that most current systems use a group of attributes contained in a credential for supplying user attributes. Attribute Trust provides a higher granularity by dealing with individual attributes. This enhances user privacy by limiting the unnecessary disclosure of attribute values. Attribute Aggregation means that any user in this system will usually have a number of attribute providers AP. While building mutual trust with a RP, the user is expected to provide a number of attributes [8]. These attributes need to be aggregated from APs. Depending on the APs' functionality, this may be generated by the user or delegated to the RP by the user. Another method is a user mediated aggregation and it is applied when the AP issues signed credentials to the user. The user can have pre-issued credentials or can request freshly signed credentials. Minimum information disclosure can be applied where the AP can provide credentials with the attribute values hashed by a one-way function [9]. The user can provide the relevant attributes to the RP in plaintext, which can be verified by the RP by hashing them with the same one-way function and comparing against the signed credential [9],[10].

II. RELATED WORKS

In [11], a proposal of a perfect decentralized access control scheme with aggregate key encryption for data stored in cloud. This scheme provides secure data storage and retrieval. Along with the security the access policy is also hidden for hiding the user's identity. This scheme is so powerful since we use aggregate encryption and string matching algorithms in a single scheme.

Manuscript published on 28 February 2015.
***** Correspondence Author (s)

Dr. Faris M. Al-Athari, is Currently Working as Professor in the College of Science and Information Technology of Zerqa University, Jordan.
Dr. Abdulameer K. Husain, he has Completed Master Degree in Computer Science, University of Sadam, Iraq.

The scheme detects any change made to the original file and if found clear the error's. The algorithm used here are very simple so that large number of data can be stored in cloud without any problems. The security, authentication, confidentiality are comparable to the centralized approaches. A research introduced the new notion of multi-attribute aggregation operator, which incorporates many standard aggregation methods, and classifies classical properties into some main groups. Different examples are provided. The researchers introduce a new concept of aggregation operators, based upon the idea that in some cases any input value may be accompanied by a set of attributes which enter the process of fusion of the data in the sense that anyone of them has the property to influence, monotonically or not, the final result of the aggregation [12]. A proposed system is discussed which is related to a privacy-preserving system using Attribute based Multifactor Authentication. This system provides privacy to user's data with efficient authentication and stores them on cloud servers such that servers do not have access to sensitive user information. Meanwhile users can maintain full control over access to their uploaded files and data, by assigning fine-grained, attribute-based access privileges to selected files and data, while different users can have access to different parts of the System. This application allows clients to set privileges to different users to access their data. [13] A research mentioned that managers of large industrial projects often measure performance by multiple attributes. So, this paper is motivated by the simulation of a large industrial project called a land seismic survey, in which project performance is based on duration, cost, and resource utilization. To address these types of problems, we develop a ranking and selection procedure for making comparisons of systems (e.g., project configurations) that have multiple performance measures. The procedure combines multiple attribute utility theory with statistical ranking and selection to select the best configuration from a set of possible configurations using the indifference-zone approach. This research applied the above procedure to results generated by the simulator for a land seismic survey that has six performance measures, and describes a particular type of sensitivity analysis that can be used as a robustness check [14]. In [15] a paper of weighted aggregation operators in multiple attribute decision making and its main goal is to investigate ways in which weights can depend on the satisfaction degrees of the various attributes (criteria). This paper proposed and discussed two types of weighting functions that penalize poorly satisfied attributes and reward well satisfied attributes. The researchers discussed in detail the characteristics and properties of both functions. Moreover, They presented an illustrative example to clarify the behavior of such weighting functions, comparing the results with those of standard weighted averaging.

III. PROPOSED SYSTEM

This work presents an authenticity method for any user that depends upon a group of his/her attributes. For this purpose we need to aggregate the most significant attributes that distinguish users to be classified to different security and authenticity levels. Also each attribute must be classified to different authenticity levels and each level has its own score. The sum of the scores determines the types of privileges and services granted to each user. To construct the system we need to build two providers in the form of secure database. The first one is called attribute provide (AP) and the second one is service provider (SP). Figure 1 illustrates the general structure of this method.

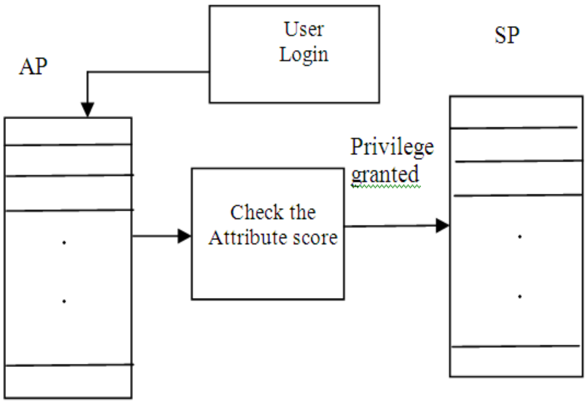
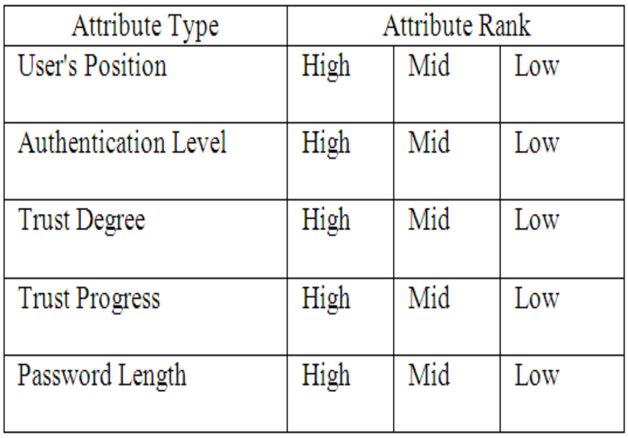


Figure 1: The general Structure of Attribute –Based Authentication.

The AP contains different levels for each attribute. Each attribute is classified as low, mid, and high and assigned a different score In this method we assign scores as follows: low =15%, mid=25% and high=60%. Figure 2 illustrates a sample of such attributes.



Attribute Type	Attribute Rank		
User's Position	High	Mid	Low
Authentication Level	High	Mid	Low
Trust Degree	High	Mid	Low
Trust Progress	High	Mid	Low
Password Length	High	Mid	Low

Figure 2: Attribute Types with Their Classes.

These attributes have been chosen because they are the best attributes which are characterized each use in a certain authenticity level. The user's position attribute give a good indication of the user importance depending on the level of the responsibilities in the organization. Each user in that position also has a level of authentication depending on the position level. We also have a test of each user to see the degree of his/her authenticity. It is necessary to examine the trust degree attribute. When the manager tests the trust degree attribute for each user, the manger must monitor the progress in trust degree in order to transit it to another secure level. Finally, the length of each user's password can be used as an important attribute for classifying users together with the previous attributes or some of the other attributes because not all users have all of the required attributes.

Figure 3 gives details of some of privileges granted to each user depending on the total scores. In this method we choose 4 principle privileges: Read (R), Write (W), Append (A) and Execute (E) and from these we can construct 2^4-1 =15 combined privileges because we ignore one of them. Note: Y means privilege type granted and N means no grant for that type of privileged.

R	W	A	E
N	N	N	Y
N	N	Y	N
N	N	Y	Y
N	Y	N	N
N	Y	N	Y
N	Y	Y	N
N	Y	Y	Y
Y	N	N	N
Y	N	N	Y
Y	N	Y	N
Y	N	Y	Y
Y	Y	N	N
Y	Y	N	Y
Y	Y	Y	N
Y	Y	Y	Y

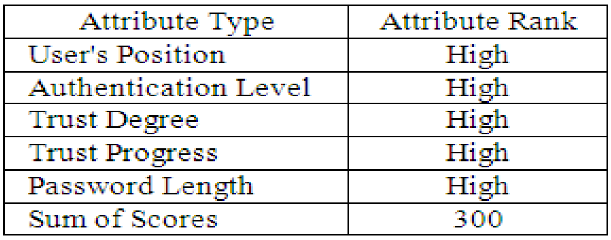
Figure 3: Privileges Granted Along with The Type of Grant.

When the system grants a privilege type, this depends on a mixture of attribute class. For example a user may be with attribute of class mid of a certain one, a low class of another attribute and may be with another mid class related to a different attribute type. The sum of these scores is calculated which from it the system grants that user the suitable one such as W privilege or a combined ones such as R/W.

In order to grant privileges, we limit the score sums of all attributes as following:
From 205 to 300, the user is granted all privileges.
From 100-120, the user is granted write/execute only.
From 80-85, the user is granted write only.
Less than 85, the user is granted read only.

IV. RESULTS

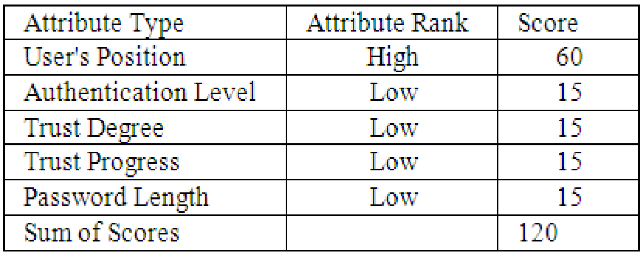
Case 1:
First we choose a user with the following attributes with type ranks for each attribute.
In this case the user gets all privileges.



Attribute Type	Attribute Rank
User's Position	High
Authentication Level	High
Trust Degree	High
Trust Progress	High
Password Length	High
Sum of Scores	300

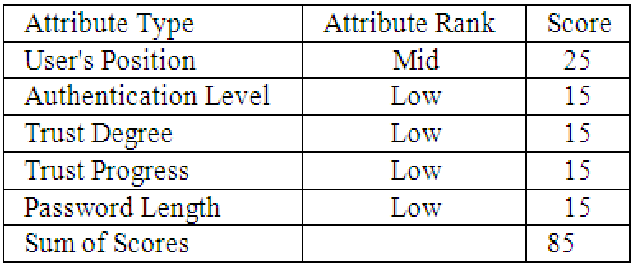
In this case the user gets all privileges.

Case 2:



Attribute Type	Attribute Rank	Score
User's Position	High	60
Authentication Level	Low	15
Trust Degree	Low	15
Trust Progress	Low	15
Password Length	Low	15
Sum of Scores		120

In this case the privileges granted are write/execute.
Case 3:



Attribute Type	Attribute Rank	Score
User's Position	Mid	25
Authentication Level	Low	15
Trust Degree	Low	15
Trust Progress	Low	15
Password Length	Low	15
Sum of Scores		85

In this case, the privilege granted is write only.

V. CONCLUSION

This scheme presents a proper authentication method by applying the most significant attributes for each user. These attributes had been selected to provide unique information of each user. The database of attributes is designed in such a way that we can maintain and update it to include other important attributes according to technology advances and the activities of some new attacks against the system. This scheme provides a strong method especially in sensitive applications. In addition, the proposed scheme can be used to grant privileges and services depending on the scores assigned for each attribute type which in turns this type is divided into specific classes .Finally, by inherent application of this method, the system manager can monitor the attributes progresses in term of evaluating user's trust within the organization.

REFERENCES

[1] Y.Eric, and T.Jin, "Attributed Based Access Control (ABAC) for Web Services ", Proceedings OF THE IEEE International Conference on Web Services (ICWS), 2005.
[2] S.V. Nagaraj, " Access Control in Distributed Object Systems: Problems with Access Control Lists", p. 163, IEEE WETICE, 2001.
[3] N.Toni, "Attribute Certificates in X.509", HUT TML 2000, Tik-110.501 Seminar on Network Security, Helsinki, Finland 2000.
[4] L.John and N. Magnus, "Attribute Certification: An Enabling Technology for Delegation and Role-Based Controls in Distributed Environments", Proceedings of the fourth ACM workshop on RBAC, pp 121 - 130, 1999.
[5] K. Reiter, and G. Stubblebine, "Authentication Metric Analysis and Design", ACM Transactions on Information and System Security, Vol. 2, No. 2, Pages 138–158, May 1999,
[6] B .Thomas, B. Malte, and K. Birgit, "Valuation of Trust in Open Network ", Proceedings of the European Symposium on Research in Computer Security U.K, 1994,
[7] W. Chadwick, "Authorisation using Attributes from Multiple Authorities ", Proceedings of the 15th IEEE International Workshops on Enabling Technologies (WETICE'06), 2006.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

[8] N. Klingenstein, "Attribute Aggregation and Federated Identity", Proceedings of the 2007 International Symposium on Applications and the Internet Workshops (SAINTW'07), 2007.

[9] V. David, M. Blough, and C .David, "Minimal Information Disclosure with EfficientlyVerifiable Credentials", appear in DIM'08 (Fourth ACM Workshop on Digital Identity Management), Fairfax, VA, USA, October 2008.

[10] A. Squicciarini, E. Bertino, E. Ferrari, F. Paci, and B. Thuraisingham, "PP-Trust-X: A System for Privacy Preserving Trust Negotiations", ACM Transactions on Systems and Information Security, July 2007.

[11] C. Ashwin, and S .Dharani , "Decentralised Access Control with Aggregate Key Encryption For Data Stored In Cloud", International Journal of Innovative Research in Computer and Communication Engineering , Vol.2, Special Issue 1, March 2014.

[12] V. Roberto, and M. Radko, "AGGREGATION WITH MULTI-ATTRIBUTES: A NEW PERSPECTIVE, 6th International Summer School on Aggregation Operators - AGOP 2011.

[13] T.Lakshmi Praveena, V.Ramachandran, and CH. Rupa, "Attribute based Multifactor Authentication for Cloud Applications", International Journal of Computer Applications (0975 – 8887) Volume 80 – No 17, October 2013.

[14] B. John, J. Morrice, and W. Mullarkey, "A Multiple Attribute Utility Theory Approach to Ranking and Selection ", Management Science © 2001 INFORMS Vol. 47, No. 6, pp. 800–816, June 2001.

[15] P. Ricardo and R. Rita , " Aggregation with generalized mixture operators using weighting functions ", Fuzzy Sets and Systems 137, 43-58, 2003.

Dr. Faris M. Al-Athari, is a professor of Mathematical Statistics and is currently working as professor in the college of science and Information Technology of Zerqa University, Jordan. He earned his PhD. from Wyoming University, USA, in 1983 and his master degree from North Carolina State University, USA in 1979. He taught at Baghdad University from October 1983 to September 1999, the Hashemite University, Jordan from October 1999 to September 2009 and joined Zarqa University in September 2009 up to date. He has published more than 40 papers in peer-reviewed articles. His teaching and research interests include the mathematical statistics, Regression and Linear Models, Stochastic Processes, and Statistical Techniques Using Computer. He got the prize of the best researcher in Zarqa University, Jordan.

Dr. Abdulameer K. Husain, Jerash University-Jordan. He has completed Master degree in computer science, university of Sadam, Iraq, in 1991 and his PhD in computer science, computer security from Al-Neelain University, Sudan. He has total 20 years teaching experience and presently working as Associate professor in Jerash University –Jordan. He has a prize of the best scientific book.