IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 4, April 2021

DOI 10.17148/IJARCCE.2021.10447

Random Password Generator

Sachin Tiwari[1], Ms Sameera khan[2]

Final Year Student, Amity school of Engineering &Technology, Amity University Chhattisgarh, Raipur, India [1]

Assistant Professor, Amity School of Engineering &Technology, Amity University Chhattisgarh, Raipur, India [2]

Abstract: The direction of computing is affected and lead by several trends. First, we have the Data Overwhelm from Commercial sources (e.g., Amazon), Community sources (e.g., Twitter), and Scientific applications (e.g., Genomics). Next, we have several light-weight clients belong to many devices spanning from smartphones, tablets to sensors. Then, clouds are getting popular due to their advantages since they are cheaper, greener, and easy to use compared to traditional systems. Finally, sensitive data stored as a plain text on a cloud system would be vulnerable to unauthorized access and the security become an important aspect. We believe that these advancements steer both research and education and will put together as we look at data security in the cloud. We introduce a password-based encryption (PBE) approach to protect sensitive data, investigate the performance metrics of the proposed approach, and present the experimental results for the key generation and the encryption/decryption calculations.

I. INTRODUCTION.

Cloud computing has been rising as one of the most robust and widespread technologies that provide access to shared resources such as CPUs, hard disks, network devices, and so on that can be automatically assigned and freed with minimum administrative work.1 clouds offer improved functionality and better cost-performance than traditional approaches in many areas of scientific research, computational science, and engineering.2 many of these opportunities have not been explored in depth as there is currently no viable business model as clouds charged as operating funds (bearing overhead) must compete with no-cost resources available through universities and federal initiatives. on general principles, one can expect clouds to be the most economical computing resource as they offer economies of scale (one has around 100 000 servers in a large cloud data-centre) and their internet access model can allow cloud-centres to be placed in optimal locations where operating costs are low and environmental impact is minimal. of course, current national supercomputer resources operate near 100% utilization (whereas clouds typically operate below full utilization allowing an attractive interactive model) and often are directly or indirectly subsidized by the host organization and this obscures the comparison of cloud and traditional scientific computing approaches.

clouds offer interesting opportunities as both infrastructure (iaas) and software (paas) levels. their software model has been designed for the wide-range data-intensive applications in the e-commerce, social media, and search fields. these have been reinforced by the commercial cloud focus as general next- generation enterprise data-centre technology.

comparing clouds, grids (distributed systems), and supercomputers, clouds have synchronization and communication costs that lie between those of distributed systems and supercomputers. further clouds tend to be optimized for external access and not for inter-node communication performance. thus, highly parallel large-scale simulations are not likely to move to clouds in the near future and should remain staple of traditional supercomputers. however, there are two important classes of applications where clouds could perform well and offer attractive cost- performance, interactive elastic (on demand) use, and powerful new software platforms.

II. THE ARCHITECTURE OF THE PROPOSED APPROACH:

figure 1 shows the overall architecture of a cloud- based system, which utilizes the proposed password- based encryption approach to secure user-related sensitive, data runs on amazon public cloud. this system consists of three main components: (a) the cloud clients; (b) the online data sources; and (c) a cloud-based federation and unification system wrapped with security module operates on amazon public cloud. the cloud clients can be any clients such as smartphones, tablets, laptop pcs, and so on that interact with the system over the http protocol. the online resources represent data sources located on the web such as repositories, scientific databases, social bookmarking, and annotation tools, and so on.

this system is a collection of services for managing social data scattered on the internet. during the deployment phase of the proposed system on the amazon cloud, the properties of the amazon public cloud have been utilized and its properties are described in detail:

1. the hardware layer: this layer is responsible for managing the physical resources of amazon public cloud such as physical servers, routers, switches, power, and cooling systems. in real life, data-centres are the places where the hardware layer is typically implemented in a data-centre generally contains around thousands of servers that are organized in racks and interconnected through switches, routers, or other components. hardware configuration, fault tolerance, traffic management, power, and cooling resource management are the typical issues of the hardware level.

2. the infrastructure layer: the infrastructure layer is also known as the virtualization layer, this layer generates a pool of storage and computing resources by partitioning the physical resources by using virtualization technologies such as xen,35 kvm,36 and vmware.37 this layer is a crucial component of cloud computing paradigm due to many key features are only made available through virtualization technologies such as dynamic resource assignment etc. amazon ec2 service has been utilized for the deployment of the cloud-based software services.

3. the platform layer: the platform layer is built on top of the infrastructure layer and it consists of operating systems and application frameworks. the main purpose of this layer is to minimize the burden of deploying applications directly into vm containers. for instance, google app engine operates on the platform layer to provide api support for implementing database, storage, and business logic of typical web applications. amazon simple db service has been used for satisfying the storage needs of the cloud-based software services.

4.the application layer: the application layer is located at the highest level of the hierarchy and it consists of the actual cloud applications. cloud applications can leverage the automatic-scaling feature to achieve better performance, availability, and lower operating cost when compared to traditional applications.34 the password-based encryption module wraps the cloud-based software services and they have been deployed as a saas model on the application layer of the amazon cloud. the security module is used for authenticating the system users and encrypting/decrypting the user-related sensitive data located on the cloud storage. the proposed approach is composed of two major parts, namely, the registration phase and the authentication/access to social websites phase. the registration phase is performed only once, and the authentication/access to social web sites phase is executed every time a user logs into the system. the proposed work does not need to store users' passwords related to users' login. in other words, there is not any password file for managing authentication process. users are authenticated through the usage of the generated encryption/decryption keys by comparing the entered usernames with the decrypted one. if the generated keys are correct which means that the entered password is also correct then the encrypted usernames will be matched. details of the authentication process is explained in section 3.2. the overall process consists of the registration, the authentication, and the usage of sensitive data and reaching sensitive data requires the cloud services to log in to remote social web tools by using the related user's credentials.

III.3.1 REGISTRATION PHASE:

this phase is invoked whenever a user registers with the remote system. the registration phase is provided through the deployed cloud-based federation and unification service system and works as follow:

- a user who wants to register; enters first name, last name, selects a username, and a password for the cloud-based system. also, the user enters the related user credentials for social web tools (sensitive data: usernames and passwords) that will be used for accessing to the remote annotation sites to retrieve data by the cloud-based services.

- the selected password by the user, automatically system generated unique salt value for each user (randomly generated number) and the number of iteration count are used through a one-way hash function to generate an encryption key. the unique salt value is stored in a database on the cloud system.

- the profile info (sensitive data: usernames and passwords) of the user for the remote annotation sites are encrypted by the generated encryption key and stored into a database on the cloud system.

- the selected username for the proposed system is also encrypted by the generated encryption key and then stored into the cloud-based system database in two forms: an encrypted and a plain format

IV.3.2 AUTHENTICATION PHASE AND ACCESS TO REMOTE SOCIAL TOOLS:

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 4, April 2021

DOI 10.17148/IJARCCE.2021.10447

this phase is invoked whenever a user wants to login to the proposed cloud-based system. after successful verification of the user, the remote system allows the user to access the system. the login and the verification phase work as follows:

• the entered username for logging into the system is compared with the one that was stored in the proposed system database in a plain format during the registration phase. if there is any match then it continues with the step 2, otherwise:

V. O THROW AN ERROR MESSAGE STATING THAT USERNAME OR PASSWORD IS INVALID.

• the entered password of the user, unique salt value retrieved from the proposed system database during the registration phase and the number of iteration count are used through a one-way hash function to generate encryption/decryption keys. the encrypted username associated with the plain username located in the cloud database is retrieved and decrypted by using the decryption key. then, it is compared with the username that is entered by the user to login:

o if the decrypted username matches with the one that is entered by the user to login, then the user is set into the session and continue as successful login. whenever the authenticated user wants to access to remote web tools, the federation and unification cloud services can access to remote sites by using the associated profile info. to do so, first, the regarding username and password pairs are decrypted through the decryption key that is automatically generated after the user authentication. then the remote social tools can be accessed and targeted metadata can be retrieved easily via the provided cloud services.

o if the decrypted username does not match with the one that is entered by the user to login, then throw an error message stating that username or password is invalid.

VI. 4.1 SYSTEM REGISTRATION AND AUTHENTICATION EXPERIMENTS:

our main goal in doing this experiment is to measure the baseline performance of the proposed security module wrapped around the cloud unification/federation prototype services deployed on amazon public cloud. in our experiments, we have used the “pbkdf2withhmacsha1” function to generate the key with “aes/cbc/pkcs5padding” option to encrypt the message with 1000 iteration. we also use the similar settings to decrypt the message. in this work, time for aes and hashing operations are not considered since they are negligible. so, we have measured the total time for password-based-encryption protocol for key generation, encryption, and decryption operations. we have tested the performance of the proposed system by measuring the time spent to generate encryption/decryption keys, encryption, and decryption of the sensitive data by using the generated keys. we have also calculated the password space and the minimum required time to break the system through the brute force attacks via the usage of a personal laptop pc with a regular graphic card and the nvidia gtx 1080 graphic card. the client programs were run on a personal laptop to make a request to access social web tools from the cloud-based system, while cloud-enabled system was running on amazon cloud. in this experiment, we were exploring the performance metrics of our methodology for “generating encryption/decryption keys”, “encryption,” and “decryption” services of the proposed password-based encryption approach. in our, each testing case, the clients send sequential requests for login standard operation resulting in generating an encryption/decryption key and encryption/decryption functions are executed 1000 times. we recorded the average time for generating an encryption key, encryption/decryption of the sensitive data, and this experiment was repeated 50 times.

VII. 4.2 SYSTEM REGISTRATION AND AUTHENTICATION EXPERIMENTS RESULTS:

we conduct experiments where we investigate the base performance of the proposed system. we have implemented the password-based encryption module in java language, using java standard edition compiler with version 1.8.0_121-b13. the configuration of the testing environment where our client code written in java language and is running to communicate the implemented services on amazon cloud is given in table 1. during the generation of the keys, encryption, and decryption operations; we have set the key length to 128 bits, salt value to 16 bits, and the iteration counter to 65 536. the test data consist of a password value (10 bytes) that obeys the rules defined in section 4.3 and a 16-bit salt value added to a user's password resulting in a total of 12 bytes. figure 4 represents the required times for basic key generation, encryption, and decryption operations of our system. in this experiment we recorded processing times for the generating encryption/decryption key, the decrypt/encrypt service to measure the processing times of the proposed service. key generation, encryption, and decryption operations are also used whenever the proposed system reaches the remote annotation sites to retrieve users' data. this experiment shows the necessary time requirements to generate a key and encrypt/decrypt operations that are necessary for major services that interacts with the online annotation systems.

VIII. 4.3 the password space and security calculations:

we assume that a password value created by a user during the registration process must be at least eight characters long and required to consist of the following characters:

- punctuations: possible 32 characters
- capital letters: possible 26 letters (a…z)
- small letters: possible 26 letters (a…z)
- numbers: possible 10 numbers (0…9)

under these assumptions, our whole password space for a minimum eight character long password will be:

on the security perspective, the nvidia gtx 1080 graphic card can perform 51 500 (∼51 × 103) pbkdf2execution per second39 whereas we can perform 10 pbkdf2 executions with our testing environment given in section 4.2. under the assumption that one nvidia titan x graphic card is used with 65 536 (∼65 × 103) iterations for obtaining the password from out of 251.68 password space, then the necessary time needed to reach the password will be:

if instead of one, 1000 of nvidia gtx 1080 graphic cards are used parallel for obtaining the password, then the necessary time needed to reach the password will be:

as a result, our proposed password-based encryption approach can guarantee the security of user-related sensitive data located on a cloud environment based on the above calculations showing the minimum required time to obtain a user's password. 4.4 benefits of the proposed work over password-based authentication:

IX. our proposed work allows users to login into the cloud system where their login credentials for social web tool can become available for accessing social web tools. after successful login to the system, encryption/decryption keys are generated for the logged user and the user's sensitive data will be accessible for being used by cloud services to communicate with the associated social web tools. the proposed work does not need to store users' passwords related to users' login. in other words, there is not any password file for managing authentication process. there exists a number of attacks in literature for password files that are used in existing password-based authentication systems (eg, brute force, dictionary etc.). it is easy to use these types of attacks in password-based authentication systems if a user's password is weak or a weak hashing algorithm is used for getting has a value of the password. on the other hand, our proposed work ensures the authentication of the users and the encryption of the user- related sensitive data located on a cloud. to provide these services, our proposed system does not contain any password file type structures. the users are authenticated when they are successfully login to the cloud system that integrates our proposed password-based encryption approach. during the authentication of the users, the encryption/decryption keys that are also used for encrypting/decrypting the users' credentials for social web tools are generated.

X. CONCLUSION

we introduced a novel architecture for a password-based encryption approach that stores data in an encrypted form on the cloud to protect the sensitive data. the password- based encryption service is an add-on architecture that runs one layer above existing information service implementations. to achieve data privacy and protection on the cloud, we have introduced and discussed our password-based encryption approach that is based on symmetric cryptosystems and provides the security of the user- related sensitive data stored on a cloud environment. the proposed work does not need to store users' passwords related to users' login. another saying is that there is not any password file for managing authentication process. users are authenticated through the various steps by password-based authentication approach using generated symmetric keys.

we performed a set of experiments to evaluate the performance of the password-based encryption service to understand whether it can achieve information encryption with acceptable costs. we shared our experiment results for required minimal timing values for security calculations and the least time to obtain a user password.

DOI 10.17148/IJARCCE.2021.10447

with this research, we discussed the proposed password- based encryption approach for a cloud-based federation/unification service framework and its ability to handle privacy and security of the user-related sensitive data. we intend to further improve this approach by focusing on the various techniques to identify the unsuccessful login tries to prevent the attackers from trying to login to the system. as the development of cloud computing technology and security issues is still at an early stage, we hope our work will provide a better understanding of the design challenges of cloud computing and security needs and pave the way for further research in this area.

REFERENCES

[1] mannan, m., van oorschot, p.c., whalen, t.: user study, analysis, and usable security of passwords based on digital objects.

[2] ieee transactions on information forensics and security 6(3-2), 970–979 (2011)

[3] 2cluley, g.: lastpass vulnerability potentially exposed passwords for internet explorer users (august 2013), https://www.grahamcluley.com/2013/08/ lastpass- vulnerability/

[4] fido alliance: fido uaf protocol specification v1.0: fido alliance proposed standard 08 (december 2014)

[5] halderman, j.a., waters, b., felten, e.w.: a convenient method for securely managing passwords. in: ellis, a., hagino, t. (eds.) proc. www 2005, may 2005. pp. 471–479. acm (2005) 5. horsch, m., h¨ulsing, a., buchmann, j.a.: palpas - passwordless password synchronization (2015), arxiv:1506.04549v1 [cs.cr], http://arxiv.org/abs/1506. 04549

[6] horsch, m., schlipf, m., braun, j., buchmann, j.a.: password requirements markup language. in: proc. acisp 2016, july 2016. pp. 426–439. lecture notes in computer science, to appear, springer-verlag (2016)

[7] karp, a.h.: site-specific passwords. tech. rep. hpl-2002-39 (r.1), hp laboratories, palo alto (may 2003)

[8] kelly, s.m.: lastpass passwords exposed for some internet explorer users (august 2013), mashableuk, http://mashable.com/2013/08/19/ lastpass- password-bug/

[9] mannan, m., van oorschot, p.c.: passwords for both mobile and desktop computers: obpwd for firefox and android. usenix ;login 37(4), 28–37 (august 2012)

[10] mannan, m., van oorschot, p.c.: digital objects as passwords. in: provos, n. (ed.) proc. hotsec'08, july 2008. usenix association (2008)

[11] mannan, m., whalen, t., biddle, r., van oorschot, p.c.: the usable security of passwords based on digital objects: from design and analysis to user study. tech. rep. tr-10-02, school of computer sciemce, carleton university (february 2010), https://www.scs.carleton.ca/sites/default/files/tr/tr-10- 02.pdf

[12] mccarney, d.: password managers: comparative evaluation, design, implementation and empirical analysis. master's thesis, carleton university (august 2013)

[13] pauli, d.: keepass looter: password plunderer rinses pwned sysadmins. the register (november 2015), http://www.theregister.co.uk/2015/11/03/keepass_ looter_the_password_plunderer_to_hose_pwned_sys_ad mins/

[14] ross, b., jackson, c., miyake, n., boneh, d., mitchell, j.c.: stronger password authentication using browser extensions. in: mcdaniel, p. (ed.) proc. 14th usenix security symposium, july/august 2005. usenix association (2005)

[15] wolf, r., schneider, m.: the passwordsitter. tech. rep., fraunhofer institute for secure information technology (sit) (may 2006)

[16] yee, k.p., sitaker, k.: passpet: convenient password management and phishing protection. in: cranor, l.f. (ed.) proc. soups 2006, july 2006. acm international conference proceeding series, vol. 149, pp. 32–43. acm (2006)