International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 9 5596 - 5599

Improved Storage Security using IDS and Performance using Container De-Duplication

Shelke Pooja H.
Computer engineering,
SND COE & RC YEOLA,
Yeola, Maharashtra, India
poojashelke93@gmail.com

Shelke Aarti H.
Computer engineering,
SND COE & RC YEOLA,
Yeola, Maharashtra, India
aartishelke94@gmail.com

Pardeshi Yogita K.
Computer engineering,
SND COE & RC YEOLA,
Yeola, Maharashtra, India
pyogita56@gmail.com

Khairnar Shweta S.
Computer engineering,
SND COE & RC YEOLA,
Yeola, Maharashtra, India
khairnarshweta6@gmail.com

Guided by:
Prof. Khumbharde M. V.
Assistant Professor Of Computer engineering,
SND COE & RC YEOLA,
Yeola, Maharashtra, India

Abstract— Due to enormous increase in use of web services in our day today life, web services have moved to multitier design where in web server runs the application front-end logic and data are outsourced to a database or file server. In our system, we will implement secure de-duplication which is a technique for eliminating duplicate copies of data, it has been largely used in cloud storage to reduce storage space and upload bandwidth with Container security, an IDS system that models the network acts as user sessions across both front-end web server and back-end database. By monitoring both the web and subsequent database requests, we are capable to search out attacks that an independent Intrusion Detection System (IDS) unable to identify. In this system, each user requesting for our application will be allocated separate container. The container based web architecture not only fasters profiling of causal mapping, but it also provides an isolation that obstruct future session hijacking attacks .Each user will hold de-key which is a new construction in which users do not require to manage any keys on their own but as an alternative securely distribute the convergent key shares across multiple servers. We implement De-key to demonstrate that De-key incurs limited overhead in realistic environments.

Keywords- De-duplication, secret sharing, multitier web application, Container Architecture, Session ID.

*****

I. INTRODUCTION

In the existing system two steps are used for avoid duplication that is file level and block level duplication detection. For considering private organization portal or social networking for our scenario we are introducing this concept. In our system we try to reduce sharing rules and user level security and duplicate post sharing.

Hence in block level or file level duplication we not need to examine. In this system we are creating one portal in that all members will shared the post such as video, text and images. So when user wants to upload any type of data this data is in encrypted format and also owner need to add Key of user's with he want to share the copy. When user want to share same copy of data to another user then he need to add keys of other user. That's why it occupied less space and it will be secured technique.

The Fig 1.1 represents container based approach of Container Architecture by using this techniques we can detect attacks in multi-tier web services. By using this approach we can also create models of regularity of isolated user session that include the both front end (Http) and back end (File or Sql) network transaction.

For accurately associates the web request with succeeding Database query we need to used container ID. Thus, also we can build a causal mapping profile by taking both the web server and Database traffic into account.

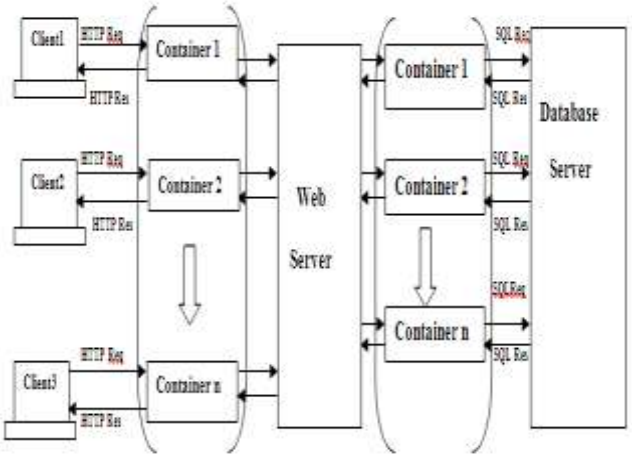

Fig 1.1 Container Architecture

II. RELATED WORK

1. In Double-Guard: Detecting Intrusions in Multitier Web Applications (2014) published by Meixing Le, Angelos Stavrou, and Brent Byung Hoon Kang, Member, IEEE [3][6], in this paper they present Double-Guard system for detect attacks in multi-tiered web services. They focus on to create normality models of isolated user sessions and also include determiner both the web frontend (HTTP) and backend (File or SQL) network transactions. To designate for each user's web session to a dedicated container, they used a lightweight virtualization technique for isolated virtual computing environment. To correctly associate the web request with the subsequent DB queries they use container ID. By taking determiner the web server and Database traffic into account hence Double-Guard can build a causal mapping profile.

2. In Secure Distributed De-duplication Systems with Improved Reliability (2015) published by IEEE and Jin Li, Xinyi Huang, Shaohua Tang,Xiaofeng Chen,Yang Xiang Senior Member, Mohammad Mehedi Hassan, IEEE and Abdulhameed Alelaiwi Member, IEEE[1][2]. to increase reliability of data when achieving the confidentiality of the user's outsourced data or lacking an encryption mechanism they proposed the distributed de-duplication systems. In this system they proposed four constructions were to support block-level and file-level data de-duplication. In this also achieved security of tag consistency and integrity. They implemented their de-duplication systems using the RSS scheme. And they also demonstrated that it incurs small encoding/decoding overhead comparative to the network transmission up above in regular upload/download operations.

3. In Using Container Architecture to Note Intrusion for Multitier Web Application(2013) publish by Manoj E. Patil Associate Professor SSBT's COE, Jalgaon Rakesh D. More Student SSBT's COE, Bambhori, Jalgaon[4]. They proposed the system which is intrusion detection system for multitier web applications that assemble normality model. This method forms container-based IDS with multiple input streams to produce alerts that are Different from previous approaches.

4. In VirtuaGuard: Intrusion Detection System on Static and Dynamic Web Applications(2013) publish by Prahsant Sonawane ,Ajinkya Nikam, Bhim Biradar, Sagar Dhere, Prof .Ruta Kulkarni Zeal Education Society's Dnyanganga College of Engineering and Research, Pune 41104[6]1. They presented Virtua-Guard approach for multitier web applications intrusion detection. the detection of web-based attacks they implemented by enlarging the general IDS. From each web-server session with a lightweight virtualization they have reached this by isolating the flow of information. They quantified the detection correctness approach when they attempted to model static and dynamic web requests with the back-end data system and DB queries. Which their experiments proved to be effective at noticing different types of attacks.

5. In Intrusion Detection Using Double Guard In Multi-Tier Architecture(1st March 2014)publish by K.Kavitha, S.V.Anandhi Student, M. E., Dept. of CSE, Dr.SACOE,Tamilnadu, India Associate Professor, Dept. of CSE, Dr.SACOE, Tamilnadu, India[6][3]. They proposed multitier web analyzer is developed to model the behavior of the web applications. The mapping model is used for observe the abnormal behavior of multitier web applications both at the front end as well as the back end data. They provides diverse session ID's for different HTTP requests which is helpful in isolating the information flow of all web server sessions, for container architecture. Hence, the multitier web analyzer is able to recognize wide range of attacks invading the system. By using lightweight virtualization they reach by isolating the flow of information from each and every web server session. Moreover, we quantified the detection accuracy of their focus on when we attempted to model dynamic and static web requests with database queries and back-end file system. In future work by using causal mapping between web request and database queries they detect and prevent sql injection attack and Privilege Escalation Attack.

III. EXISTING SYSTEM

By using the technique of secret sharing a file is first divide and encoded into fragments, instead of encryption mechanisms. These shares will be contributed across multiple independent storage servers. Furthermore, to manufacture for De-duplication, a small Cryptographic Hash-value of the content will also be computed and sent to each storage server as fingerprint of fragment stored at each and every server. Only the data owner who first uploads the data is essential to estimate and allocate such secret shares, while all users who own the same data copy do not need to evaluate, and store these shares anywhere. To recover data copies, users must have to access a less amount of storage servers through authentication and derive the secret shares to rebuild the data. In other words, the secret shares of data will exclusively be accessible by the authorized users who own the corresponding data copy.

Implementation of De-duplication systems using the RSS scheme that enables high reliability and confidentiality levels. Our results demonstrate that the new proposed constructions are efficient and the redundancies are optimized and approximate with other storage system provide for the same level of reliability.

When user uploading data system generates one encryption key for document and encrypt whole file. Then user again encrypt this key by his master key and then while sharing in social network or with any friend that time one more key will be generated and add this key in key management table because of that countless duplicate keys are store for some data .for example for 1 TB data there would be 10GB space required for only key storing at destination end user will extract this data by his master key.

A. Limitations

If user dropped his master key he not once get that data or unable to share as well. This system requires large memory space for storing multiple keys and also master key.

IV. PROPOSED SYSTEM

We are avoiding this kind of multiple keys storing and also master key issues. We are just adding reference of key while sharing data so no need to keep master key for every transaction. Once it will be shared to any one automatically reference key will link to share user. So at destination user will gate data by without providing any key but in background keys are applied already.

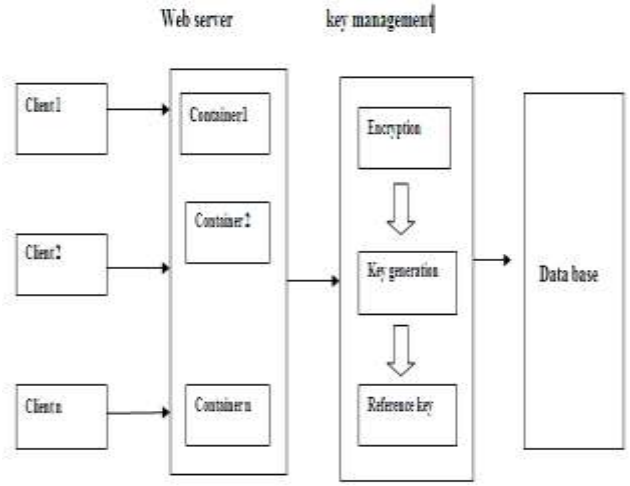

Fig 4.1 proposed system

According to existing system we are providing more security using Double Guard technique. Double-Guard is a system used to recollect attacks in multitier web services. Our focus on can create normality models of isolated user sessions that include both web front end (http) and back end (My Sql) network transactions.

It will employ a technique to assign each and every user's web session to a dedicated container which is an isolated virtual computing environment. We use Container ID to without error associate the web request with the subsequent DB queries. Thus is can construct a causal mapping profile by grasping both the web server and DB traffic into account. So after completing the Double-Guard Process de-duplication process will be start and We are creating one portal where all member will sharing the post like text, images, and video. So whenever they will upload any data it will be in encrypted format and owner need to add Key of user's with he want to share the copy. So whenever any user will share the same copy to another user he just needs to add keys of other user. And it will be secured as well as less space consuming technique. We are managing the security department wise, every department having their own Convergent key and all users having master key to access their data on server.

A. Advantages

In this system, each user requesting for our application will be allocated separate container. The container based web architecture is not only quickly profiling of causal mapping, but it also provides an isolation that avoid future session-hijacking attacks. Each and every user will hold dekey which is a new construction in which users do not need to organize any keys on their own but rather securely distribute the convergent key shares across multiple servers. We implement Dekey to demonstrate that Dekey incurs limited overhead in realistic environments.

V. MATHEMATICAL MODEL

Let S be a system that find out duplicate copies of the file using Authorized de-duplication system in hybrid cloud.

S={F,O,B,C,T,P,M}

Where,

F={F1,F2,F3,…Fn}

F1={B1,B2,B3,…Bn}

B1= {CBi,TBi,Pki}

CB i= Set of cipher text File

T = Token [16- Bit , unique token for File]

P= Private Key (PKi) used for encryption & description mechanism

Venn diagram

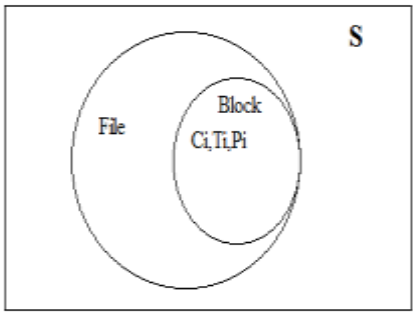

Fig for: **F∩(BU(C,T,P))**

VI. CONCLUSION

We designed a system which achieves confidentiality and also enables block-level de-duplication at the same time. Our system is built on top of convergent encryption. We showed that it is worth performing block-level de-duplication as an auxiliary of file level de-duplication since the gains in terms of storage space are not affected by the overhead of metadata management, which is minimal. Additional layers of encryption are added by the server and the optional HSM. As the additional encryption is symmetric, the impact on performance is negligible. We also showed that our design, in which no component is completely trusted, prevents any single component from compromising the security of the whole system. In this system, each user requesting for our application will be allocated separate container. The container based web architecture not only quickers the profiling of causal mapping, but it also provides an isolation that prevents future session-hijacking attacks. Each user will hold dekey which is a new construction in which users do not need to supervise any keys on their own but instead securely distribute the convergent key shares across multiple servers. We implement the Dekey that incurs limited overhead in realistic environments.

REFERENCES

[1] Jin Li, Xiaofeng Chen, Mingqiang Li, Jingwei Li, Patrick P.C. Lee, and Wenjing Lou, "Secure De-duplication with Efficient and Reliable Convergent Key Management",IEEE Transaction on parallel and Distributed system, VOL. 25, NO. 6, JUNE 2014.

[2] Jin Li, Xiaofeng Chen, Xinyi Huang, Shaohua Tang and Yang Xiang Senior Member, IEEE and Mohammad Mehedi Hassan Member, IEEE and Abdulhameed Alelaiwi Member, IEEE "Secure Distributed De-duplication Systems with Improved Reliability", IEEE Transactions on Computers Volume: PP Year: 2015.

[3] Meixing Le, Angelos Stavrou, Member IEEE, and Brent ByungHoon Kang, Member IEEE, "DoubleGuard: Detecting Intrusions in Multitier Web Applications", IEEE Transactions on dependable and secure computing, VOL. 9, NO. 4, MARCH 2014.

[4] Manoj E. Patil Associate Professor SSBT's COE, Bambhori, Jalgaon Rakesh D.More Student SSBT's COE, Bambhori, Jalgaon,"Using Container Architecture to Detect Intrusion for Multitier Web Application", International Journal of Computer Applications (0975 – 8887) Volume 62– No.9, January 2013.

[5] Ajinkya Nikam, Bhim Biradar, Sagar Dhere,Prahsant Sonawane Prof .Ruta Kulkarni Zeal Education Society's Dnyanganga College of Engineering and Research, Pune 411041, "VirtuaGuard: Intrusion Detection System on Static and Dynamic Web Applications", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 1, January 2013.

[6] K.Kavitha, S.V.Anandhi Student, M. E., Dept. of CSE, Dr.SACOE, Thiruchendur,Tamilnadu, India Associate Professor, Dept. of CSE, Dr.SACOE, Thiruchendur, Tamilnadu, India, "Intrusion Detection Using Double Guard In Multi-Tier Architecture", International Journal of Innovative Research in Computer and Communication Engineering(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014.

[7] Mark W. Storer Kevin Greenan Darrell D. E. Long Ethan L. Miller Storage Systems Research Center University of California, Santa Cruz {mstorer,kmgreen,darrell,elm} @cs.ucsc.edu, "Secure Data Deduplication".

[8] Chilla.Santhi, A. Satya Mallesh Dept. of CSE, Bonam Venkata Chalamayya Engineering College ., Odalarevu-Amalapuram E.G.dt,AP, India, "Intrusion Detection in Web applications Using Double Guard", International Journal of Research in Computer and Communication Technology, Vol 2, Issue 12, December- 2013.

[9] Nita Prakash Saware1, Manish Umale2, Nidhi Maheswarkar3 1, 2 (Department of Computer Engineering Lokmanya Tilak College of Engineering Koparkhairane, Mumbai, 3(Department of Computer Engineering, Dhyanganga College of Engineering Narhe, Pune, "Detecting Intrusions in Multitier Web Applications.", Nita Prakash Saware, Manish Umale, Nidhi Maheswarkar / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 3, Issue 4, Jul-Aug 2013, pp.2007-2014.

[10] Chilla.Santhi, A. Satya Mallesh Dept. of CSE, Bonam Venkata Chalamayya Engineering College ., Odalarevu-Amalapuram E.G. India "Intrusion Detection in Web applications Using Double Guard", International Journal of Research in Computer and Communication Technology, Vol 2, Issue 12, December- 2013