Improved Security of Data in Cloud Network to Prevent Detect Key Recovery Attacks Using Node Creation for Authentication

Adya Zizwan Putra
Teknik Informatika, Universitas Prima Indonesia
* adyazizwanputra@unprimdn.ac.id

Abstract - The use of internet in the past decade has increased rapidly people using it for transmission of data saving their works, storing all the private information in a system and transmitting through internet. Due to high usage of internet there is also possibility of losing data by unauthorized access and getting hacked and misuse of data. Previously there was a method used known as kids, but the problem with this method was the method used for generation of key and keeping it secrecy, the attackers could easily get access to the key after black box attack. In this paper the proposed system helps to provide more security and prevents it from attacks and also protect the data stored in the system. The proposed schema can be implemented in hospitals for health care domain, for saving the data of Patience by using cloud storage by using it in the detection system. Many developers and researched have introduced schemes in Machines learning and one of this scheme was key based detection system, But this system required more security to prevent from the attackers, in the proposed module am using cryptographic algorithm for creating secret key and for saving the data and Bowl Fish algorithm to hide the data from the attackers and recover the key from the AES algorithm which is saved in encrypted format which has steps of verification to recover the key and give prevention against unauthorized usage and it provides security from the attackers by saving all the data of patience in a hospital using different domains kept in cloud platform.

1. Introduction

In present the use of internet usage is increased and the number of people using internet technology to send and receive, communications in this there is the possibility for the data to be misused by hackers who authenticate through an unauthorized access to improve the protection of the system for better security previously there was many methods proposed such as intrusion detection system which use to monitor all the activities from the main network and inform all the details to the main system. The detection includes abstracting various behaviors of the system by using predefined rules and comparison of same data that could provide result in the main system[2].

The concept of machine learning is a big sector in which it has task related to identifying scam various malwares and security related to network [3]. The problems related to machine learning is specifically is of algorithm ad existence of consistency of adaptive usage of intelligence for having better performance to detect a breach in a system. Usually this detection system has two types known...
as Network Based a, Host Based The network base is related to the network to perform detection activity on the various servers and where as host base used to monitor single host or a particular server. In this we introduced key based system to have better security and prevention from attacks caused by hackers this method depends on generation of a key and keeping the secrecy for the generated key. With this type of method attackers use to easily interact with the system, so there’s a need for improvement in key based system to have better security and more reliability from Grey box attacks[1].

In this proposed system it gives better security and more reliability to store data on the network by prevention of various attacks in by using the data which is saved using different domains in a cloud storage

2. Literature Review
The use of internet for various purposes has been increased where millions of people are getting connected through inter to communicate and have data storage inside a cloud which has services like data transfer from one person to another person using internet. For this the network connection has become an evaluating aspect for connection between users by authenticating and reaching the end users easily without harming both users and preventing attackers from not accessing information of an organization for different reasons of an organization.

Therefore, preventing security in networking is a crucial factor. To have better security for a network, detection system is used for monitoring unusual activities and taking action over it. If incase the hacker get to know the rules or the algorithm which is been used the hacker can create an another new algorithm to attack the system, for this there is a requirement for improving key improving and better security to store the data in the form of encrypted and the keys are only based detection system in which the need to know the behavior of secret key, but the issue with this key based system is the attackers get to know the key after having inter action with the system, therefore there is a need for known to the authorized user to have access and maintaining confidentiality[2].

The research done by different research and developers shows that the problem of security is not only related to learning of algorithm but also creating security web by formulating higher upgraded security features by involving different types of methods for handling data by using algorithms such as game theoretical and improving the traditional way of recognizing the algorithms by having better distribution of data set which helps in assumption of malicious user who cannot manipulate the data and reduce the performance of the system[3].

The attackers does not require a module, but they only observe a specific loop inside an algorithm, for this purpose reverse engineering has been developed to observe the complexity of find an malicious user in this the classifier used in the training data set the attacker might know the space but also must include the positive and negative aspect of an algorithm by which this query detection is easier to find out the attacker and improve the security by using queries in the reverse engineering specially using it inside a featured space[4]. Introduced polymorphic based detection which helps in prevention of attacks by matching enumeration of single occurrence inside a profile and this method is used as a systematic way to issue warnings for attacks that can be identified under any circumstances [5].

It uses byte frequency based detection system and there were many applications which was developed to supervise the pay load of a packet to identify any kind of anomaly [6], Developed 4 modules in an individual approach to find out and have detection by checking length of the character, grammar, token finder which helps in detection of HTTP attacks, for this purpose, Developed PAYL to record various frequency inside a packet inside a packet for an each individual byte which computes several profiles and clustering was used to decrease number of profiles and instead checking byte frequency, they developed a byte model but it has a disadvantage that the attacker can invade if he has a knowledge of IDS [7].An analytical experiment using a frame work which provide information which is hidden by using the evasion of classifier, all the hidden information and the method of implementation using different classifiers they develop key base secret key which helps in monitoring
network anomalies this proposed method has three steps of implementation which includes training mode- which checks for the byte and detection mode which checks the word frequency count and count according to number of sets and key selection is used for detection and maintaining quality of key based detection system [8].

3. Problem and Proposed System

In the existing system the model used doesn’t meet all the security requirements and attackers could easily recover the key and interact with the system which leads to misuse of user data and scamming for this there is a need for having better data security by ensuring integrity with reliability of access control by improving key based detection system. Aim is to provide better security by stopping attackers to regain the key which be in any form of settings inside a network.

The absence of security for detecting unauthorized inside a network by key recovery from any kind of classifier depending on the data to measure the attacks and prevent it from future encounter by hackers by improving counter measures inside a frame work that could include setting up of length of words in larger format and our aim is to security features for the key based intrusion detection system by improving data security by using a secure cloud storage for the use of different health care domains to retrieve and access the data for a particular patient or staff in a health care management system.

Proposed System Modules and Architecture, In the proposed module I introduced node creation for authentication which is needed to be created for each user using the network in which the system gets all the details about the user and store the data provided sing predefined rules after the node is created and saved in the data base to retrieve the saved file in an encrypted format the user needs to have a secret key for each file for opening in the network. The misuse of data by the attackers is a main concern for the user to secure the network there is a need for secret key that ensures data files to be protected and modified for a particular authenticated user by using grey box attacks which happens in the secret key and is modified at the end node.

The need of detection for the key based system for authentication, there is need for alerts in the main system and to check the activity of the users who have authenticated for the network, if any unspecified access is found the key based detection system modifies the key and then regain the access provided to the internal node.

In the proposed system I am using cryptographic algorithm for creating secret key and for saving the data and Bowl Fish algorithm to hide the data from the attackers and recover the key from the AES algorithm which is saved in encrypted format which has steps of verification to recover the key and

![Figure 1. Secret Key based Architecture](image-url)
give prevention against unauthorized usage and it provides security from the attackers by saving all the data of patience in a hospital using different domains in the cloud.

**AES Algorithm** Implementing AES algorithm secret keys are generated. Consider the normal text, initial state as \( x \) by performing ADD operation by \( X \)-ors keys in round within the state (figure 1). The initial round-1, is initiated by operating substitution known as Sub Bytes implementing S-box; Permutation of shifting Rows are initiated on every state; and Mix Columns function is initialized, and then provides AddRoundKey for performing the first stage and \( Y \) is defined as cipher text and the state (Figure 1).

**Blowfish Algorithm:**

Save uploaded file data using blowfish algorithm (figure 1).

Divide \( X \) into two 32-bit halves: \( xL, xR \)

For \( i = 1 \) to 16:

- \( xL = XL \oplus P_i \)
- \( xR= F(XL) \oplus xR \)
- Swap XL and xR
- Swap XL and xR (undo the last swap)
- \( xR = xR \oplus P_{17} \)
- \( xL= xL \oplus P_{18} \)
- Recombine \( xL \) and \( xR \)
- Share the secret Key
- Share the secret key with authenticated node
- Find hidden Internal collision
- Compare the \( K = K \)

**Recovering the Key**

Solution perspective for scheme studied

\( S = \{ s,e,X,Y,fm\} \)

Initial state (s): User.
Exit/End state (e) : success or failure

Input (X):

- \( X1 = User \) credentials \( X2= user \) data

Output (Y):

- \( Y1= secret \) key for each user
Algorithm (fm):
1) Secret key created using AES algorithm
2) Data save in encrypted format using blowfish algorithm
3) Share the secret key
4) Find internal collision

4. Analysis Results
The key based detection system it does node authentication for each set of node in this process the user can able to upload a data file and give secret key for all the individual files used in the network with the help of secret key user can access the data if hackers use black box attacks the system alerts about the attacks and gives instructions by giving information for preventing training data which is needed to be implemented to show the performance about the hack time and recovery time I plotted a graph for time calculation which shows the hackers need more time to attack the system while the recovery key used in this gives complexity and security and less time to recover the key from that of hacking time. The performance of the system is shown in the form of graph for the time taken for each process for individual files (Figure 2).

| File | Upload Time (smt) | Hack Time (smt) | Recovery Time (smt) |
|------|-------------------|-----------------|---------------------|
| File 1 | 196              | 486             | 176                 |
| File 2 | 168              | 352             | 171                 |
| File 3 | 155              | 581             | 156                 |
| File 4 | 142              | 454             | 120                 |
| File 5 | 528              | 470             | 124                 |
| File 6 | 373              | 522             | 138                 |
| File 7 | 176              | 414             | 135                 |
| File 8 | 229              | 380             | 123                 |
| File 9 | 325              | 472             | 216                 |
| File 10 | 237             | 478             | 209                 |

Table 1. System overall performance.
5. Conclusions

The use of different algorithms and predefined rules which was used previously in the detection systems to prevent hacking from the attackers but to overcome the issues related to security different machine learning schemes were previously used one of such scheme is key based detection system. It is a method in which it generates the key and keep the secrecy of the key. But the problem with this was attackers could easily attack the network using black box attacks for this there was need in improvement in security system provided by this detection module so we proposed cryptographic algorithm and Blow Fish algorithm which helps to improve security and confidentiality of data over cloud this implemented technique helps in protecting against black box attacks which also helps in increasing security in the system and helps the user to save the data in an encrypted form and gives protection against unauthorized access in the network.

References

[1] A Scarfone, Karen; Mell, Peter (February 2007). "Guide to Intrusion Detection and Prevention Systems (IDPS)" . Computer Security Resource Center (National Institute of Standards and Technology) (80094). Retrieved 1 January 2010.
[2] R. S. Mrdovic and B. Drazenovic, “KIDS-Keyed Intrusion Detection System” Proc. Seventh Intl Conf. Detection of Intrusions and Malware,and Vulnerability Assessment (DIMVA 10), pp. 173-182, 2010.
[3] N. Dalvi, P. Domingos, Mausam, S. Sanghai, and D. Verma, “Adversarial classification,” in 10th ACM SIGKDD Intl Conf. on Knowl. Discovery and Data Mining, 2004, pp. 99108.
[4] D. Lowd and C. Meek, “Adversarial Learning”, Proc. 11th ACM SIGKDD Intl Conf. Knowledge Discovery in Data Mining (KDD 05), pp. 641-647, 2005.
[5] O. Kolesnikov, D. Dagon, and W. Lee, “Advanced Polymorphic Worms: Evading IDS by Blending in with Normal Traffic”, Proc.USENIX Security Symp.2005.
[6] C. Kruegel and G. Vigna. “Anomaly detection of web-based attacks” In Proceedings of ACM CCS, pages 251-261, 2003.J. G
[7] K.Wang and S. Stolfo. “Anomalous payload-based network intrusion detection”. In Recent Advances in Intrusion Detection, 2004.
[8] B. Biggio, G. Fumera, and F. Roli, “Adversarial Pattern Classification Using Multiple Classifiers and Randomisation”, Proc. IAPR Intl Workshop Structural, Syntactic, and Statistical Pattern Recognition, pp. 500-509, 2008.
[9] Aarti Devi, Ankush Sharma, Anamika Rangra “A Review on DES, AES and Blowfish for Encryption & Decryption” International Journal of Computer Science and Information Technologies, Vol. 6 (3) , 2015, 3034-3036.
[10] Yufen Shen “The Implementation of Anti-attack AES Mathematical Model in Library Network Encryption” 2nd International Conference on Computer and Information Application (ICCIA 2012).
[11] Don Coppersmith1 , Lars R. Knudsen2 , and Chris J. Mitchell3 “Key recovery and forgery attacks on the MacDES MAC algorithm” IBM Research, T.J. Watson Research Center, Yorktown Heights, NY 10598, USA.
[12] Juan E. Tapiador, Agustin Orfila, Arturo Ribagorda, and Benjamin Ramos Key- Recovery Attacks on KIDS, a Keyed Anomaly Detection System” IEEE transaction on DEPENDABLE AND SECURE COMPUTING, VOL. 12, NO. 3, MAY/JUNE 2015.
[13] P. Mell and T. Grance, The NIST Definition of Cloud Computing, version 15, October 7, 2009, National Institute of Standards and Technology (NIST), Information Technology Laboratory (www.csrc.nist.gov).
[14] S.M. Khan and K.W. Hamlen, Anonymous Cloud: A data ownership privacy provider framework in cloud computing, in Proc. of IEEE 11th International Conference on Trust, Security
and Privacy in Computing and Communications (TrustCom), 2012.

[15] S. Subashini and V. Kavitha, A survey on security issues in service delivery models of cloud computing, in Proc. of Journal of Network and Computer Applications, pp.1-11, 2011.

[16] F. Jun et al., Analysis of integrity vulnerabilities and a non-repudiation protocol for cloud data storage platforms, in Proc. of 39th International Conference on Parallel Processing Workshop, 2010.

[17] AhmedESandASaeedR 2014A Survey of Big Data Cloud Computing SecurityInternational Journal of Computer Science and Software Engineering (IJC SSE)78-85