International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 04 | Apr 2019 www.irjet.net p-ISSN: 2395-0072

Security from threats of computer system

Samiksha Kamble[1], Sanyukta Khobragade[2], Ankita Lajurkar[3], Rutika Ganjiwale[4]

[1,2,3,4]*Student, Dept. of CSE, Prof. Ram Meghe Institute of Technology and Research, Badnera, Maharashtra, India*

Abstract - *Governments are finding cyber security a major challenge given that they store far more data than the private sector but often in older and vulnerable systems. They are regularly targeted not just by opportunistic hackers but also by teams funded and trained by other nations as has become evident in the latest outbreak of malware threat. They are looking for secure and productive technologies to ramp up systems against phishing, dangerous exploits, advanced Threats like sophisticated malware and zero-day threats. Today cloud computing is used in industrial field. To overcome this Cloud facilitates its users by providing virtual resources via internet. Security of cloud-based applications is one of the key concerns of cloud customers. Advance threat prevention must be designed so the government data can be sandboxed on government owned private cloud itself for data. Analysis of these solutions can be used to determine the lacunae in the data security issues which are nothing but drawbacks.*

Key Words: **Malicious Software1, Encryption2, Decryption3, Heuristic detection technique4, Signature based detection5**

1. INTRODUCTION

Governments are finding cyber security a major challenge given that they store far more data than the private sector but often in older and vulnerable systems.

Zero day attack is random attack which cannot be eradicate, it only can identify and avoided, it is also called one day attack, and it is a threat, exploit computer application and vulnerabilities, as this attack occurs on day zero awareness. The developers had zero days to address and patch[1].

Cloud design is a blossoming and rapidly evolving model, with new features and capabilities. Security of cloud-based applications and data is one of the key concerns which should be monitored while operating. Secure software and secure software life cycle management are basic fundamental operation require for the protection of cloud services.

The systems rest on the ancient principles of confidentiality and integrity, but applied to distributed, virtualized, and dynamic architectures of a system. This paper presents an analysis of security issues in a cloud environment. Solution exists for a few. Analysis of these solutions can be used to determine the lacunae in the data security issues which are the drawbacks in the system.

There are many different threats to computer systems and the data stored on them in memory[2]. These threats increased considerably and computers started to be networked with the Internet, it has become one of the most important considerations in managing a computer system.

There are many different threats to computer systems and the data stored on the system. These threats increased drastically computers which are networked with the Internet, they have become one of the most important considerations in a computer system. Some of them are hacker, malwares i.e. malicious software, viruses, worm, spyware, phishing, public wifi access.

2. LITERATURE REVIEW

Data security is main part in todays world. There are many different types of threats are rising nowadays which can harm the data. Hence it is necessary to provide security from these attacks to data.In 2013, Mohammed Hassouna, Nashwa Mohamed, Bazara Barry and Eihab Bashier et.al proposed, in this section, an explanation on how electronic mailing systems work is provided. The explanation is largely based on parts from

Email System: Components and Protocols: The two primary message sections are the header and the body. The header section contains the vital information about the message including origination date, sender, recipient(s), delivery path, and format information. The message body contains the actual information of the message.

Existing Schemes to Secure Email Systems are emails have become official communication technology and sensitive documents can be attached to them. Therefore, it is necessary to provide the basic security services, namely, authentication, confidentiality, integrity by email systems to insure security and privacy. Most of the existing mailing systems enable users to access their emails with usernames and passwords, which is called password authentication method.

Certificateless Public Key Cryptography (CLPKC): The concept of Certificateless Public Key Cryptography (CL-PKC) to overcome the key limitation of the identity-based cryptography. In CL-PKC a third party called Key Generation Center (KGC) supplies a user with partial private key. The user then combines the partial private key with a secret value that is unknown to the KGC to

obtain his/her full private key. This way the KGC does not know users private keys which is hidden. Then, the user combines the same secret value with the KGC's public parameters to compute his/her public key.

In 2015, Meltem Kurt Pehlivanoğlu, Nevcihan Duru et.al proposed, In the literature there are some designs of secure email based system. Lu and Geva [6] describe the implementation of a distributed search engine called SEGPX depend on secure email communication. It uses X.509 Public-key and attributes certificate frameworks and utilizes email servers for communications with receipent. RC4 algorithm is used because it focuses on WEP protocol security. MRC4 uses the same key scheduling algorithm (KSA) with RC4 but with two different keys and two different S boxes (S1 and S2).

3. SECURITIES FROM THREATS

Security can be provided to these threats by using following mechanism.

3.1 Username and password 1

A username is a computer identity given to people in an organization so that they can use the computer system. It uniquely identifies the user to the system so that only their files and other shared resources that the systems administrator has permitted can be seen.

Passwords are used to make the system secure and prevent access from unauthorized users. Passwords should only be known to the account holder and changed regularly for safety. Once someone other than the account holder knows a password, it can be changed and the genuine user of the account can be denied access by forget password.

3.2 Firewalls 2

A firewall is a part of a computer network that is designed to block unauthorized access from people outside the organization while permitting authorized communications inside the organization to the outside world.

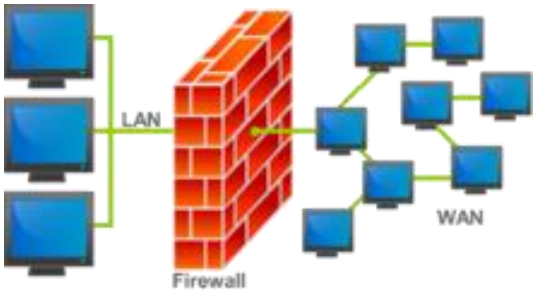


Fig-1: Firewall Protection

Firewalls can be implemented in either hardware or software, or a combination of both or individually. Firewalls are frequently used to prevent unauthorized Internet users and information from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria will be discarded.

3.3 Email Encryption 3

This is used to protect data while it is being transmitted over the Internet or used to protect important data stored on a computer. Un-encrypted data is very easy for people to read especially when it is being transmitted over telephones lines that are used by most people to connect to the Internet. Encryption works like this: Each character is scrambled according to a secret code known to the account holder.

The coded character is then stored or transmitted in place of the original character.

When the data is needed it is converted back using the same encryption key used to create data.

3.4 Anti-virus Software 4

Viruses are the biggest threat and these days, anti-virus software will include protection from adware, spyware, viruses, anti-spam and also include a firewall.

There are two ways protection is provided:

3.4.1 Method 1

When the software is installed, the administrator will decide what events are to be monitored. For example downloading files from the Internet, opening a memory stick, checking the address etc. The software then scans the files to see if any of the contents match signatures of viruses stored in its database. If they do, they will be blocked from use or the virus element deleted from database. The user will also be alerted that a virus has been found in the data. As new viruses are found, updates will be made available to the anti-virus program because it is important that is kept up to date, otherwise known viruses could get through and infect the computer and damage the files.

3.4.2 Method 2

When unusual activity is detected. For example a program that would not normally download a file from Internet begins to do. If this activity matches a rule in the database about a known virus, the transfer will be blocked by the admin.

3.5 Backup 5

Files can also become corrupt as re result of programs crashing, power failures or malware. It is important then that computer users and business computer users in particular, have protection against these situations by having adequate backup copies of all files. Backup is a file that can be used to replace the original in the case of the original being lost or corrupted.

Proposed System:

Data Security is explained with the help of its threat and security. In username and password it is mandatory to provide correct details. This is used to protect data whilst it is being transmitted over the Internet or used to protect important data stored on a computer. For email encryption various algorithms can be used such as AES and RC6.

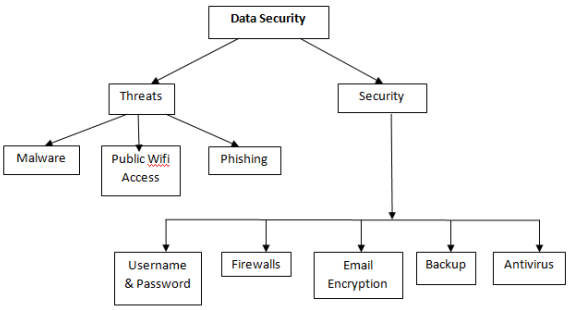
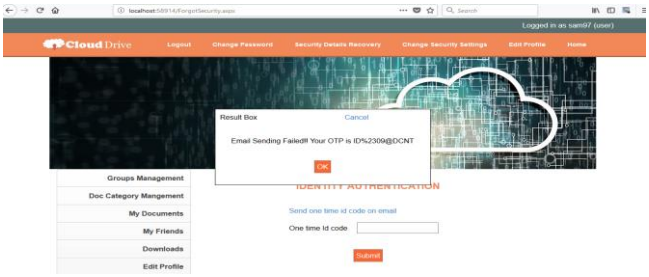


Fig -2: Flow Diagram

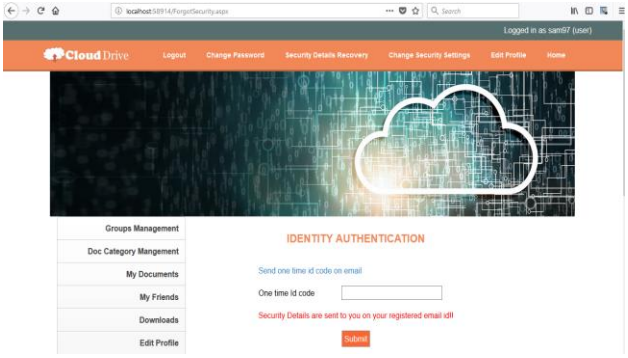
AES algorithm work on key and provide more security. One of the primary advantages of AES is its ubiquity that data will be sent securely with authentication. The three possible key lengths supported by AES allow users to pick a tradeoff between speed and security.RC6 is safe, it can prevent Brute Force (128 Bit = 2^128 attempts). RC6 is simple, compact and secure block cipher. Backup of data helps from system recovery. Antivirus is necessary to protect system from viruses.

The zero-day attacks occur between the time period, when vulnerability is first exploited and when software vendors start to develop a counter to that attack. A firewall is designed to block unauthorized access from people outside the organization while permitting authorized communications inside the organization to the outside world.



Screenshot 1: OTP send through mail

While authenticating to users identity the system can send the OTP through mail to user. That OTP will be placed by user into system and by this system will authenticate user.



Screenshot 2: User authentication

User will provide OTP into this block and then system will check the OTP whether it is correct or not. If it is correct, system will allow user to change details.

4. CONCLUSIONS

In the paper "Cost effective on cloud solution for zero day attack prevention" aims to provide Cloud facilitates its users by providing virtual resources via internet. Security of cloud-based applications and data is one of the key concerns of cloud customers when dealing with security measures. Advance threat prevention sandboxed on government owned private cloud itself for data. Analysis of these solutions can be used to determine the lacunae in the data security issues.

This means that there is increased demand for zero day attack detection and prevention solution that can provide exact results. Producing such a solution can be quite difficult, requiring a considerable investments as well as mature engineering team experienced in kernel and user level endpoint monitoring and general cyber security techniques and algorithms which can be understandable.

Hence, finally we are going to provide security to different important files, documents and database using

different security algorithm and by using cloud and try to prevent threat of zero day attack.

REFERENCES

[1] Aparna Verma, M.S.Rao, A.K.Gupta, W. Jeberson, Vrijendra Singh, "A literature review on malware and its analysis", Central Forensic Science Laboratory, Hyderabad, A.P., India ,Gujarat Forensic Science University, Gandhi Nagar, Gujarat, India, Department of Forensic Science, SHIATS, Allahabad U.P., India, Department of Computer Science and IT, SHIATS, Allahabad, U.P., India, Indian Institute of Information Technology, Allahabad, U.P., India

[2] Dolly Uppal, Vishakha Mehra and Vinod Verma, "Basic survey on Malware Analysis, Tools and Techniques", Department of Computer Engineering, Rajasthan Technical University, Kota.

[3] Velte, Tata McGraw- Hill Edition "Cloud Computing – A Practical Approach" (ISBN-13:978-0-07-068351-

[4] Garima Gupta, P.R.Laxmi and Shubhanjali Sharma," A Survey on Cloud Security Issues and Techniques" Department of Computer Engineering, Government Engineering College, Ajmer.

[5] Kunwar Singh Vaisla1 and Reenu Saini2 "Analyzing of Zero Day Attack and its Identification Techniques" - 1Associate Professor, 2M.Tech Student, 2Department of Computer Science & Engineering, BT Kumaon Institute of Technology, Dwarahat, District–Almora, Uttarakhand, India.

[6] Dennis Distler, Charles Hornat,"Malware Analysis: An Introduction GSEC" Gold Certification, December 14, 2007

[7] Bojan jovicic, Dejan simic,"Common web application attack types and security using asp.net", University of Belgrade.

[8] Mike Ter Louw, Jin Soon Lim, and V.N. Venkatakrishnan," ExtensibleWeb Browser Security" , Department of Computer Science, University of Illinois at Chicago

[9] Meltem Kurt Pehlivanoğlu, Nevcihan Duru," Email Encryption using RC4Algorithm" Department of Computer Engineering Kocaeli University Kocaeli, Turkey

[10] Umesh Kumar Singh, Chanchala Joshi, Suyash Kumar Singh," Zero day Attacks Defense Technique for Protecting System against Unknown Vulnerabilities", Volume-5, Issue-1, pp.13-18, February (2017).

[11] Niti Sharma, "Secure Mailing System" Student, Computer Science and Engineering, Delhi Institute of Technology Management &Research, Faridabad, India

[12] Mohammed Hassouna, Nashwa Mohamed, Bazara Barry and Eihab Bashier, "An End-to-End Secure Mail System Based on Certificateless Cryptography in the Standard Security Model" Faculty of Computer Studies, National Ribat University,Faculty of Mathematical Sciences, University of Khartoum, Faculty of Sciences and Arts, University of Albaha.

[13] Toizo anan, "Paper encryption technology".

[14] BRIAN D. FINLAY,"PUBLIC THREATS, PRIVATE SOLUTIONS" Meeting Nonproliferation Challenges with the Force of the Market for security.

[15] Kunwar Singh Vaisla and Reenu Saini," Analyzing of Zero Day Attack and its Identification Techniques" February 2014.