Detecting and Preventing Transport Layer Attacks in Cloud Storage using Homomorphic Linear Authentication

K.Vijaya
B.E., M.E
Computer science and engineering,
Velalar College of engineering and Technology, Erode–638012

Brindha M
Computer science and engineering,
Velalar College of engineering and Technology, Erode–638012

Govarthini K
Computer science and engineering,
Velalar College of engineering and Technology, Erode–638012

Mathialagan K
Computer science and engineering,
Velalar college of engineering andTechnology, Erode–638012

Abstract-Cloud storage provides a convenient, massive, and scalable storage at low cost, but data privacy is a major concern that prevents users from storing files on the cloudtrustingly. One way of enhancing privacy from data owner point of view is to encrypt the files before outsourcing the moon to the cloud and decrypt the files after downloading them. However, data encryption is a heavy overhead and data retrieval processing cur's complicated communication between the data user and cloud. Normally with limitedbandwidth capacity and limited battery life, these issues introduce heavy overhead to computing and communication as well as a higher power consumption for users, which makes the encrypted search over cloud using very challenging. For optimal use of BWSN resources and to reduce the latency of BWSN users, the BWSN computing model extends the services such as networking facilities, computational capabilities and storage facilities based on demand. Due to the dynamic behaviour, distributed paradigm and heterogeneity present among the processing elements, devices and service-oriented pay per use policies; the BWSN computing environment is having its availability, security and privacy issues. This problem was solved by creating a firewall using homomorphic linear authentication. Index terms-BWSN, dynamic behaviour, service oriented and homomorphic linear authentication

I. INTRODUCTION

Distributed Denial of Service (DDOS) Attacks pose a serious threat to the cloud storage. We know that the Internet's Vulnerability to Bandwidth Distributed Denial of Service (BWDDOS) Attacks, where many hosts send a huge number of packets exceeding network capacity and causing congestion and losses, thereby disrupting legitimate traffic. TCP and other protocols employ congestion control mechanism that response to losses and delays by reducing network usage, hence their performance may be degraded sharply due to such attacks. Attackers may disrupt connectivity to servers, networks, autonomous systems, or whole countries or regions; such attacks were already launched in several conflicts. BWDDOS employed relatively crude, inefficient, 'brute force' mechanism; future attacks may be significantly more effective, and hence much more harmful. To meet the increasing threats, more advanced defences should be deployed. This may involve some proposed mechanism (not yet deployed), as well as new approaches.

II LITERATURE REVIEW

1. PRIVACY PROTECTION AND DATA SECURITY IN BWSN COMPUTING : A SURVEY, CHALLENGES AND SOLUTIONS

Privacy and security are the most important issues to the popularity of BWSN computing service. In recent years, there are many research schemes of BWSN computing privacy protection based on access control,

attribute-based encryption (ABE), trust and reputation, but they are scattered and lack unified logic. In this paper, we systematically review and analyze relevant research achievements.The architecture, concepts and several shortcomings of BWSN computing, and propose a framework of privacy protection; second, we discuss and analyze basic ABE, KP-ABE (key policy attribute-based encryption), CP-ABE (ciphertext policy attribute-based encryption), access structure, revocation mechanism, multi-authority, fine-grained, trace mechanism, proxy re-encryption(PRE), hierarchical encryption, searchable encryption(SE), trust, reputation, extension of tradition access control and hierarchical key; third, we propose the research challenge and future direction of the privacy protection in the BWSN computing; finally, we point out corresponding privacy protection laws to make up for the technical deficiencies.

2. A SECURE ACCESS CONTROL MODEL FOR E-HEALTH BWSN

In the contemporary digital era, access control is one of the security issues in the modern Electronic Healthcare System (EHS). In particular, the E-Health BWSN (EHC) needed a secure and reliable access control to access the EHC resources. In the past, several attempts have been made to provide secure and reliable access control (AC) to the EHS.This paper discussed several security problems present in the BWSN-based e-healthcare system. The security requirements and threat analysis of the EHS give an idea about developing a new security model, which is capable of handling all the aspect.

3. REPUTATION-AWARE TRUST AND PRIVACY-PRESERVATION FOR MOBILE BWSN COMPUTING

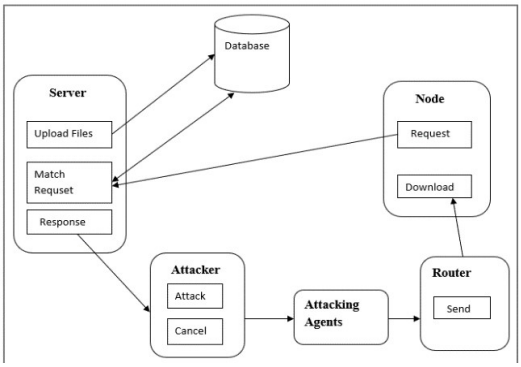
Mobile BWSN Computing (MCC) is getting growing interest due to its wide applicability in variety of social, industrial, and commercial mobile applications. Mobile and smart devices can share complex computational operations with BWSN Service Providers (CSPs). It also provides storage, access polices enforcement, and security operations. In many cases, CSP requires services from crowd contributors CCs for data collection, sharing, and mobile application support. It requires trust management for CCs to guard against malicious CCs and ensure security and privacy of data. However, end users or data requesters also demand reliable security solutions for sharing their data or accessing data from unknown CCs. To ensure strong security, mobile devices are not computationally feasible to perform complex cryptographic operations for desired privacy. To resolve these issues, we propose Reputation-aware Trust and Privacy Preservation scheme for MCC.

4.A PRIVACY-PRESERVING FOG COMPUTING FRAMEWORK FOR VEHICULAR CROWDSENSING NETWORKS

Recently, the study of road surface condition monitoring has drawn great attention to improve traffic efficiency and road safety. As a matter of fact, this activity plays a critical role in the management of the transportation infrastructure. Trustworthiness and individual privacy affect the practical deployment of the vehicular crowdsensing network. Mobile sensing as well as contemporary applications is made use of problem solving. The fog computing paradigm is introduced to meet specific requirements, including mobility support, low latency, and location awareness. The fog-based vehicular crowdsensing network is an emerging transportation management infrastructure. Moreover, the fog computing is effective to reduce the latency and improve the quality of service. Most of the existing authentication protocols cannot help the drivers to judge a message when the authentication on the message is anonymous. In this paper, a fog-based privacy-preserving scheme is proposed to enhance the security of the vehicular crowd sensing network.

III. PROPOSED METHODOLOGY

A novel approach to the cloud computing is improved by enhancing the security is proposed in this paper. Byemploying efficient modified-sha256 algorithm based on machine learning approach DDoS attacks can be efficiently handled in the BWSN computing environment. When flooded traffic found in network then immediately it is been analyzed. The attacks will be identified and immediate response will be taken to drop the malicious traffic. To adapt to these patterns, machine learning algorithms are used by the BWSN networks. This algorithm makes use of various techniques based on signature tokens which leads to the formation of decision tree to identify the attacks automatically and effectively



IMPLEMENTATION METHODOLOGY

BWSN computing is a revolution in IT technology that provides scalable, virtualized on-demand resources to the end users with greater flexibility, less maintenance and reduced infrastructure cost. These resources are supervised by different management organizations and provided over Internet using known networking protocols, standards and formats. The underlying technologies and legacy protocols contain bugs and vulnerabilities that can open doors for intrusion by the attackers. Attacks as DDoS (Distributed Denial of Service) are ones of the most frequent that inflict serious damage and affect the BWSN performance. In a DDoS attack, the attacker usually uses innocent compromised computers (called zombies) by taking advantages of known or unknown bugs and vulnerabilities to send a large number of packets from these already-captured zombies to a server. This may occupy a major portion of network bandwidth of the victim BWSN infrastructures or consume much of the server's time.

UPLOAD DATA OR FILES:

In computer networks, to upload can refer to the sending of data from a local system to a remote system such as a server or another client with the intent that the remote system should store a copy of the data being transferred, or the initiation of such a process. Where the connection to the remote computers is via a dial-up connection, the transfer time required to download locally and then upload again could increase from seconds to hours or days. A Server creates its own database then uploads its files.

USER MANAGEMENT

Often Nodes and servers communicate over a computer network on separate hardware, but both node and server may reside in the same system. A server host runs one or more server programs which share their resources with nodes. A node does not share any of its resources, but requests a server's content or service function. Nodes therefore initiate communication sessions with servers which await incoming requests. The server component provides a function or service to one or many nodes, which initiate requests for such services. A web server serves web pages and a file server serves computer files. A shared resource may be any of the server computer's software and electronic components, from programs and data to processors and storage devices.

BW-DDOS ATTACK DETECTION

In this module attacker intrudes server's response, and generate huge number of fake packets to the victim. Then it can forward this fake packet through its attacking agents. These attacking agents may be zombies or puppets or root zombies.These attacking agents again forward this fake packet to victim through router. Here router act as BW-DDOS attack detector.First router checks packets size. If huge number of packets are detected it will give the defense against this BW-DDOS attacks. Else it will forward to the requested node.This router using four types of defense mechanisms: filtering, rate limiting, detouring and absorbing, and breakthrough. It applies any one defense mechanism and get original packets.Finally, our router will forward the original packet to the requested node.

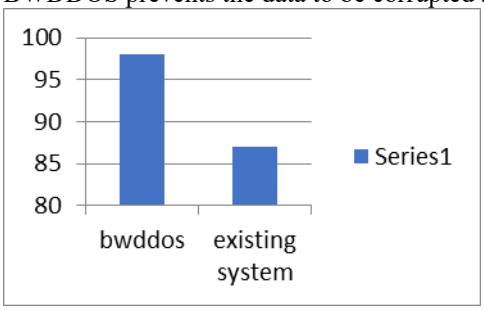
SIGNATURE AND TOKEN ANALYSIS

Clients and servers exchange messages in a request-response messaging pattern. The client sends a request, and the server returns a response. This exchange of messages is an example of inter-process communication. To communicate, the computers must have a common language, and they must follow rules so that both the client and the server know what to expect. The language and rules of communication are defined in a communications protocol. the mechanism of blockchain and proposed a modified SHA256 security protocol through smart contract to secure online transaction procedure specifically based on Blockchain Mechanism. It focus on the discussion of modifying security protocol specifically designed for

practical applications of blockchain with particular reference to privacy and trust.Here the server extracts from its database and match the node request then send this particular file to node.

IV. EXPEREMENTAL SETUP

The experimental setup proposes the result with the existing and proposed model to provide the BWDDOS prevents the data to be corrupted so that the user cannot download it.



There are various defence mechanisms, which can be deployed at different network locations. A defence mechanism can be deployed close to the destination, that is, by the victim. Note that defence mechanisms close to the destination may get a good idea about some attack's properties, but for mitigation of BWDDoS they might not be the well positioned, since many packets already get discarded near the victim. Hence, many defence mechanisms try to mitigate the attack closer to its sources.

V. CONCLUSION AND FUTURESCOPE

It is compared with conventional detection algorithms that utilize only the distribution of the number of lost packets, exploiting the correlation between lost packets significantly improves the accuracy in detecting malicious packet drops. Such improvement especially visible when the number of maliciously dropped packets is comparable with those caused by link errors. To correctly calculate the correlation between lost packets, it is critical to acquire truthful packet - loss information at individual users. Auditing architecture developed that ensures truthful packet - loss reporting by individual nodes.

In future work, this issue would be thought of about bringing down framework proficiency in various domains of military, pharma, IT sectors. This methodology is planned for the enciphering and translating of text-based information and there is no thought of the picture situated informational collection yet. We would like to propose a multi-keyword search scheme to perform encrypted data search over mobile cloud in future. As our OPE algorithm is a simple one, another extension is to find a powerful algorithm which will not harm the efficiency. Likewise, the proficiency of the proposed work can be additionally improved by the reconciliation of quantum registering to make it more versatile for portable and savvy gadgets.

REFERENCES

[1] Singh, U. Chandra, S. Kumar and K. Chatterjee, "A Secure Access Control Model for E-health BWSN," TENCON 2019 - 2019 IEEE Region 10 Conference (TENCON), Kochi, India, 2019, pp. 2329-2334.
[2] C.Nagarajan and M.Madheswaran - 'Experimental verification and stability state space analysis of CLL-T Series Parallel Resonant Converter' - Journal of ELECTRICAL ENGINEERING, Vol.63 (6), pp.365-372, Dec.2012.
[3] G.Neelakrishnan, K.Anandhakumar, A.Prathap, S.Prakash "Performance Estimation of cascaded h-bridge MLI for HEV using SVPWM"SurajPunj Journal for Multidisciplinary Research, 2021, Volume 11, Issue 4, pp:750-756
[4] P. J. Sun, "Privacy Protection and Data Security in BWSN Computing: A Survey, Challenges, and Solutions," in IEEE Access, vol. 7, pp. 147420-147452, 2019.
[5] C.Nagarajan and M.Madheswaran - 'Performance Analysis of LCL-T Resonant Converter with Fuzzy/PID Using State Space Analysis'- Springer, Electrical Engineering, Vol.93 (3), pp.167-178, September 2011.
[6] Nagarajan, G.Neelakrishnan, R. Janani, S.Maithili, G. Ramya "Investigation on Fault Analysis for Power Transformers Using Adaptive Differential Relay"Asian Journal of Electrical Science, Vol.11 No.1, pp: 1-8, 2022
[7] W. Ahmad, S. Wang, A. Ullah, Sheharyar, Z. Mahmood, "ReputationAware Trust and Privacy-Preservation for Mobile BWSN Computing," in IEEE Access, vol. 6, pp. 46363-46381, 2018.
[8] C.Nagarajan and M.Madheswaran - 'Stability Analysis of Series Parallel Resonant Converter with Fuzzy Logic Controller Using State Space Techniques'- Taylor & Francis, Electric Power Components and Systems, Vol.39 (8), pp.780-793, May 2011.
[9] G.Neelakrishnan, R.S.Jeevitha, P.Srinisha, S.Kowsalya, S.Dhivya, "Smart Gas Level Monitoring, Booking and Gas Leakage Detector over IOT" International Journal of Innovative Research in Science, Engineering and Technology, March 2020, Volume 9, Issue 3, pp: 825-836
[10] W. Jiannan, W.Xiaojie, L. Nan, Y. Guomin, M. Yi, "A Privacy Preserving Fog Computing Framework for Vehicular Crowdsensing Networks" (2018). Faculty of Engineering and Information Sciences, vol. 6, pp. 43776-43784, 2018.

[11] M. Zekri, S. E. Kahlil, N. About bit and Y. Saadi, "DDoS attack detection using machine learning techniques in BWSN computing environments," 2017 3rd International Conference of BWSN Computing Technologies and Applications (BWSNTech), Rabat, 2017, pp. 1-7.
[12] Moustafa, N. and Slay, J., "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). IEEE Military Communications and Information Systems Conference (MilCIS), pp. 1-6, (2015).
[13] R.Srinivasan, G.Neelakrishnan, D.Vinoth and P.Iraianbu, "Design and Implementation of Novel Three Phase Multilevel Inverter for Smart Grid" International Journal of MultidisciplinaryEducational Research, jan 2020, Volume 9, Issue 1(3) pp: 125-135
[14] C.Nagarajan and M.Madheswaran - 'Experimental Study and steady state stability analysis of CLL-T Series Parallel Resonant Converter with Fuzzy controller using State Space Analysis'- Iranian Journal of Electrical & Electronic Engineering, Vol.8 (3), pp.259-267, September 2012.