International Journal for Multidisciplinary Research (IJFMR)

E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Enhancing Data Protection and Compliance Through Cloud Security Solutions

Aishwarya Jagadish[1], Anusha Paniraj Shanbhog[2]

[1,2]Student, Department of Computer Science, Dayananda Sagar College of Engineering

Abstract

Cybersecurity is the practice of protecting critical systems and sensitive information from digital attacks. It provides measures to combat threats against networked systems and applications (internal as well as external) that attempt to access, change, or destroy data, extort money from users or the organization or aim to disrupt normal business operations. With recent breaches and technological attacks, maintaining cloud security has become foremost concern for business worldwide.

Keywords: Cyber Security, Cloud Computing, IoT, Cloud Forensics

Introduction

Cybersecurity is based on the CIA triad i.e. Confidentiality, Integrity and Availability of data and information. A strong cybersecurity strategy has layers of protection which includes Critical Infrastructure Security, Network and Application Security and Cloud Security. Cloud security specifically deals with true confidential computing that encrypts cloud data, at rest and in motion to support customer privacy, business requirements and regulatory compliance standards. Cloud data security is critical since most organizations use cloud computing in one form or the other. So, to maintain customer's trust and protecting assets, it is very important to prevent leaks and data theft.

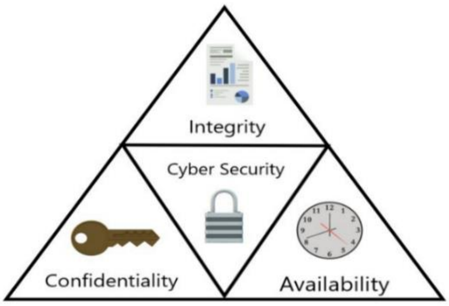

Fig 1: CIA triad

Types of Security Threats

A cyber security threat refers to any possible malicious attack that tries to illegally access data, critical information or disrupt digital operations. Cyber threats can originate from various sources like corporate spies, hacktivists, terrorist groups, hostile nation-states and criminal organizations.

The CIA Triad access to important network components or covertly obtain information by transmitting data from hard drive.

Certain types of security breach is listed below

1. Malware: It is a malicious software such as spyware, ransomware, viruses and worms which gets activated when a user clicks on a malicious link or attachment, that leads to installing dangerous software in the user's device. Once the malware is activated, it can install additional harmful software, disrupt parts making system inoperable.
2. Ransomware: It is a specific type of malware, which works by encrypting key files on a machine or network, then demanding a payment to make the files accessible again. It is a very disruptive form of attack. In some cases, a ransomware attack may make it impossible to access critical business information, or block vital system files that prevents a computer from booting up altogether.
3. Phishing: This is a cybercrime in which targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords. This information is then used to access important accounts and results in identity theft and financial loss.
4. SQL injection attack: It is a common attack vector that allows users with malicious SQL code to access hidden information by manipulating the backend of databases. This data includes sensitive business information and private customer details. A successful SQL injection attack can not only allow criminals to steal or modify data but also help them gain control over administrative access.
5. Man in the Middle attack: In this, the attacker puts himself in between the sender and the receiver to disrupt the communication flow. He manipulates both parties and achieves access to the data that the two people were trying to deliver to each other. For example, to intercept financial login credentials, a fraudulent banking website can be used between the user and the real bank webpage.
6. DoS and DDoS attack: The denial of service (DoS) attack is used to disrupt the availability of a website and not allow legitimate users to access it. Distributed denial of service (DDoS) is a type of DoS attack in which attackers compromise a large number of computers or other devices, and use them in a coordinated attack against the target system. These attacks launch a denial of service to capture the attention of security staff and create confusion, while they carry out more subtle attacks aimed at stealing data or causing other damage.
7. DNS attack: DNS Attack is a type of cyber-attack that exploits the weakness or vulnerability in a Domain name system. Attackers take advantage of the plaintext communication between clients and the DNS servers or by logging in to a DNS provider's website with stolen credentials and redirect DNS records.

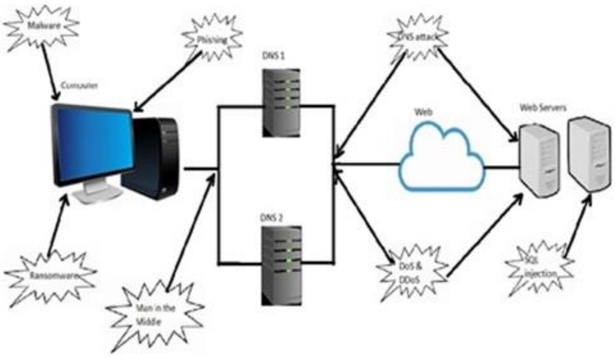

Fig 2: Types of attacks

Multi Facade of Cyber Security

Healthcare: Cloud computing can dynamically deploy virtual resources according to users' requirements for resources and computing power, without being limited by physical resources. The core technologies involved in modern medical treatment are technologies such as sense, communications, information and security. The patient information model is established through cloud computing technology to give a portrait of the patient so as to better understand the patient. It is very hard to keep sensitive and heterogeneous data obtained from wearable devices secure. So, a new cloud-based user authentication scheme is used for secure authentication of medical data. First, a successful mutual authentication between a user and wearable sensor node is done where both establish a secret session key that is used for future secure transmission of information. The authentication scheme in [1] has 7 steps-setup, registration, pre deployment, logic and authentication, password change, smart card revocation and a wearable sensor. Formal security is ensured using Real-Or-Random (ROR) model and verified using AVISPA tool and informal security is used to make sure it is resistant to different kinds of attacks. This technology is cheaper, more effective and secure.

The longstanding constraints of computational capability and storage space on mobile devices can be alleviated by outsourcing computation or data-intensive tasks to remote cloud centres. Hence, mobile cloud computing (MCC) has been recognized as a promising approach to provide pervasive healthcare services to people in their everyday life. As a result, new optimization strategies have been explored and studied to help mobile cloud healthcare services to be deployed in a more effective manner.

The integration of cloud computing with mobile phones is known as Mobile Cloud Computing (MCC) [2]. As MCC can offer significant benefits like expanded battery life, high-level storage capability, scalability and adaptability. In spite of the various advantages of using Mobile Cloud Computing (MCC) in healthcare, its growth is being hampered due to privacy and security issues. There is a need to secure Health Information worldwide, regionally, and locally and it is very important to prevent security breaches. To overcome this, Modular Encryption Standard (MES) is used, which is a modular symmetric cryptographic algorithm. It is based on the layered modeling of the security measures. Using this mechanism, Health Information can be stored securely and confidentially. MES has three main steps involved i.e. Identification (distinguishing the criticality and sensitivity of HI), Classification (selecting the degree of secrecy based on the nature of the record) and Securing (includes remaining cryptographic steps). Comparative results show that this scheme outperforms other commonly used techniques in the MCC environment. Some drawbacks of this model are: there is no consideration of image-oriented data set yet, and sometimes layered security model might may sometimes lower system efficiency. This can be improved in the future by integrating quantum computing and using block chain model for privacy.

Based on MCC infrastructure, physiological signals and vital signs collected from wireless body area networks (WBAN) could be transmitted to either the public cloud or the private cloud through smartphones or computers. It generates the healthcare data analysis results, depending on the urgency of the patient's condition, which could either trigger the alarm to physicians or be stored in the medical database for future access. It is an ideal platform that enables users to share, transmit, and process Electronic Health Record (EHR) and personal medical images.

The mobile cloud services for healthcare could be grouped into two categories, mobile cloud computing and mobile cloud storage for healthcare. Offloading the execution of computationally intensive tasks from mobile to cloud can alleviate the mobile devices from performing complicated, energy consuming jobs and thus extend the limited battery life of mobile devices. Many researchers have provided analysis [9] towards the mobile cloud offloading cost from the energy perspective, especially when the network condition deteriorates significantly.

MCC-based healthcare applications could be categorized as follows-

- Electronic Health Record (EHR) – It provides an organized approach, which collects the health information of patients and population utilizing an electronic digital format. It proposed a middleware to facilitate efficient processing of medical data synchronization with minimal latency.
- Picture Archiving and Communication System (PACS) - It is a medical imaging technique, which enables an efficient method for storing and sharing medical images across manifold modals of source machine. It is a self-adaptive method to enable high resolution medical images retrieved and transmitted over network in a reliable way.
- Tele monitoring and bio-signal processing – It is a vehicular social network established to collect and process diverse sensing data, so that safety improvement service was delivered in a real-time manner. A non-contact Electrocardiogram (ECG) measurement system was also established relying on mobile cloud infrastructure.
- Multi-Agent Medical Consultation - MCC has been utilized to provide multi-agent medical consultation services. A multi-agent mobile cloud system was designed to enable doctors, nurses and other medical staff to cooperate efficiently with each other in healthcare service provision.

Cloud computing has superior computational capability, elasticity and scalability becomes an indispensable part in MCC. It consists of the Core Cloud, the Edge Computing servers and the local cloudlets. To enhance the computational capabilities of mobile devices, a multilevel MCC infrastructure based on the granularity of different cloud resources is designed. This reduces cloud reaction time and increase energy saving. Mobile Edge Computing (MEC) could allow services to be provided close to users by taking advantage of resources nearby. It offers high-quality services to mobile users with minimized timing delay and energy consumption.

Radiation dose verification problem arises for the tumor patients and the modern medical data processing system constructed by cloud computing technology is used to solve this kind of problem. The medical industry is a special industry that is closely related to the people’s livelihood and their lives. With the introduction of information technology [10] in the medical industry, the information and automation of the medical industry have been continuously improved.

The highly intelligent and highly automatic system computing capability ensures that users can always access the services they need, and realizes the functions of self-detection, self-location and self-healing of the system. Cloud computing includes six characteristics which are virtualization technology, dynamic scalability, on-demand deployment, high flexibility, high reliability and high cost performance.

With the vigorous development of Ubiquitous Network, this environment provides infrastructure support for the realization and popularization of modern medical treatment. Modern medicine is a wireless network composed of physical data collection nodes on the human body and biosensor nodes in the human body. It has great application significance and needs in telemedicine and home domain health systems, and is becoming a strategy in the medical and communications industry. Hadoop is a widely used distributed system, and it is the basic skeleton in the existing cloud computing ecosystem. The cluster has high-speed parallel computing performance and large data storage capacity of terabyte-level data storage.

The experimental data was used to verify the accuracy of the cloud computing-based tumor medical data processing system. When the experimental method cannot measure the exposure dose of the internal organs of the human body, computer simulation can be used for calculation. By adopting a cloud-based virtualization solution, all medical management systems are sequentially migrated to the cloud data centre, which has a significant impact on the efficiency of IT maintenance staff, the utilization of hospital infrastructure, the continuity of medical system operations, and data security.

The experimental results show that the construction and application of a tumor medical data processing system based on cloud computing can better combine the individual condition and disease characteristics of tumor patients, give an accurate radiation dose for tumor pain treatment, and reduce the incidence of risk events. It has improved the standardization of tumor pain treatment by nearly 15% on average, and the treatment plan satisfaction has increased by nearly 20%.

Cloud Enabled IoT Architecture: While traditional information cybersecurity revolves around software and how it is implemented, security for IoT adds an extra layer of complexity as the cyber and the physical worlds converge. Although IoT devices may seem too small or too specialised to be dangerous, there is real risk in what are really network-connected, general purpose computers that can be hijacked by attackers, resulting in problems beyond IoT security. Once attackers have control, they can steal data, disrupt delivery of services or commit any other cybercrime they would do with a computer. Cloud has made IoT more secure with preventive, detective and corrective controls. It has enabled users with strong security measures by providing effective authentication and encryption protocols. Based on Multifactor Authentication and Lightweight Cryptography scalable and secure Big Data IoT System is achieved. A secure and decentralized Cloud Enabled Intelligent IoT Architecture using a Cipher Block Chaining Support Vector Machine is enabled.

The Internet of Things devices are increasing in number and also a lot of sensors composes the IOT leading to limited computational capability. But there a few drawbacks namely the limitation of storage capacity and security vulnerabilities. As a result, in order to overcome these drawbacks, cloud computing is used. Cloud computing domain provides reliable [13] security in terms of data processing and storage and guarantees information protection with respect to data confidentiality, availability and integrity.

An IoT-Cloud environment consists of an embedded system, sensors, core, data centre and cloud. Such an IoT-Cloud environment can use resources efficiently based on the sharing of IoT resources and in this way physical resources can be virtualized. An IoT-Cloud environment has advantages in terms of availability and efficiency but has issues such as reliability and security. Communication from device objects to the cloud service and also safe accessibility and connectivity must be provided.

A typical application area of such an IoT-Cloud technology is a smart-grid environment. The security threats that can occur are DoS attack, Message forgery, Malicious codes and control signal change. External attacks use programs other than the targeted file, including a Trojan horse, virus, or worm. Such attacks are analysed and used for the construction of an ontology for security context in a power IoT-Cloud environment.

Integrating IoT and cloud computing is a very effective approach to store and manage big data but this also has a lot of security problems. To overcome this, multifactor authentication and lightweight cryptography encryption schemes can be used [3]. The sensitive and non sensitive data are encrypted using different schemes like RC6 and Feistel scheme and are stored in private and public cloud respectively. In addition to this multifactor authentication is used to improve security of cloud. During login, data users send their registered credentials to the Trusted Authority (TA). The TA provides three levels of authentication to access the stored data: first-level authentication - read file, second-level authentication - download file, and third level authentication - download file from the hybrid cloud. The final performance is evaluated using computation time, encryption time, decryption time and security strength.

Cloud computing is an emerging technology that has majorly transformed the storage of data and accessing of applications. A variety of computing resources like servers, databases, networks and applications are provided by the Cloud. The following model [4] provides computationally secure key generation to protect the data via encryption. This key generation is based on three cryptographic algorithms including the Optimization Algorithm. An SVM based encryption service mode is constructed to minimize empirical errors. This model can withstand attacks like Chosen Cipher Attack, Chosen Plain text Attack. Statistical and differential attacks can be prevented, when images are fed to this model. This model has a higher efficiency and security

Forensics: Cloud Forensics refers to the application of digital forensics process in cloud computing environments where we need to analyze the input. It is an intelligent evolution of digital forensics that defends against cybercrimes. Forensic issues that arise in this include jurisdiction, multi-tenancy and dependency on CSPs. Hence it is very important to have a decentralised and secure evidence collection and preservation system and to secure the logs and data related to the investigation and to prevent Privacy Leakage in Cloud Environment.

The Evidence Collection and Provenance Preservation in IaaS Cloud Environment can be done using SDN and Blockchain Technology. Using the fast-growing Software-Defined Networking (SDN) and Blockchain technology for Infrastructure-as-a-Service (IaaS) cloud [5], decentralised evidence collection and preservation is made possible. Evidence is collected and stored in the blockchain which is decentralised and can be accessed by multiple people. Secure Ring Verification based Authentication (SRVA) scheme is used to ensure the security. To strengthen the cloud environment, secret keys are generated using Harmony Search Optimization (HSO) algorithm. On the basis of sensitivity level, data is ciphered and is securely stored in a cloud computing environment. A method called Sensitivity Aware Deep Elliptic Curve Cryptography (SA-DECC) algorithm is used for ciphering the data stored in the blockchain. Each evidence is stored in an individual block that is part of the SDN controller. In each block, SHA-3 based Merkle tree construction ensures the integrity of evidence. The results of this technology is more effective than centralized forensic system. This can be further strengthened by using network security within SDN.

In the field of forensics, user activity logs can be a valuable source of information in cloud forensic investigations. It is important to make sure they are reliable and secure. To achieve this, the Cloud Log Assuring Soundness and Secrecy (CLASS) can be used. In this [6], threats faced include modification of logs, repudiation of ownership of logs and violation of privacy but it is secure as it achieves the three properties of cryptography, confidentiality, integrity, and authenticity. Logs are encrypted using the individual user's public key so that only the user is able to decrypt the content. This method proposes a bloom filter-based PPL, which can be used to obtain the membership information of (Rabin's) fingerprint of chronologically ordered log chain of an epoch to prevent unauthorized modification of the log. Correctness of the log is checked and verification of PPL is carried out. A pair of keys is mutually chosen by both, the user and the CSP. This key is referred to as the content concealing key (or CC-key) as it is essential to hide user's log content. Certain rules have to be followed while using this key. Using the fingerprint of all the log chains in an epoch and single bloom filter per fingerprint decreases false positive results as well as computation time. By using this method, the verification time is significantly reduced.

Activity logs of cloud users being crucial evidence to prosecute a suspect, can reveal the actions taken by a user using cloud infrastructures. However, collecting logs from the cloud infrastructure is extremely difficult and currently investigators need to depend on CSP (Cloud Service Providers) for this and this method does not ensure confidentiality and integrity of the logs. Possible attacks include Log modification, Privacy violation and Repudiation by user or CSP. The SecLaaS scheme [7] stores logs securely, provides APIs to forensics investigators, and verifies the integrity of logs. The secrecy of logs is safeguarded by authorizing only the investigators or the court authority to access the logs by the RESTful APIs that are obtained using SecLaaS. The integrity of the logs can be made secure by the hash-chain scheme. Additionally, an auditor can check the integrity of the logs using the Proof of Past Log PPL and the Log Chain LC. Currently, two accumulator schemes i.e. Bloom filter and RSA accumulator are being used to build the proofs of past logs. In this method, a new accumulator scheme – Bloom-Tree, a variation of Bloom filter that has an enhanced and efficient performance as compared to the above methods is employed.

In order to conduct privacy leakage analysis in cloud specifically, a multi-granularity privacy leakage forensics method is used to analyse privacy violations caused by malware in cloud environment. A typical paradigm of cloud forensics follows four stages of operations which are evidence source identification and preservation, forensic data collection, forensic data examination and analysis, evidence reporting and presentation. The cloud forensics approaches are divided into three categories namely Log-based approaches, Product based approaches and VMI-based approaches.

The proposed Privacy Violation Detection System (PVDS) is a customized system for privacy detection caused by malware in cloud. It can be divided into four phases. The first phase of is where the interception of suspicious malware takes place. We intercept executable binaries from cloud and then adopt YARA to identify and classify malware samples. Cloud environment simulation is our second phase where once a suspicious binary is discovered, the virtual machine which downloads the binary will be simulated to ensure the security and privacy of user information. The third phase is when a coarse-grained forensic analysis method known as continuous RAM mirroring technique is used to do forensics and analysis. A fine-grained forensic method is introduced in the fourth [11] phase to track the propagation of user privacy. Finally, a report with respect to privacy leakage paths and behaviours is generated and retained as evidential data.

The evaluation results to validate the effectiveness of PVDS is to introduce the experimental datasets and describe some state-of-the-art malware detection tools to conduct a comparative analysis with PVDS. The coarse-grained forensic analysis and fine-grained privacy leakage detection results are reported. The experimental evaluation shows that PVDS could detect more privacy leakage paths and behaviours, especially regarding keylogger, sensitive file and memory.

The evaluation results show the usability and effectiveness of the system in privacy leak detection but it still has some limitations. PVDS could do forensic analysis in keystroke leak, sensitive memory leak and sensitive files leak, but sensitive memory area is limited and privacy leakage paths cannot cover all privacy leakage situations. Thus, more privacy leakage paths need to be added in the future.

Cloud Security

A wireless sensor network consists of a large number of miniature sensor nodes that capture a large amount of data which suffer from low quality of service due to the large amount of raw data present. To overcome this, wireless network is integrated with cloud computing forming a new computing paradigm known as sensor-cloud. It offers numerous benefits such as flexibility, scalability, collaboration, automation, virtualization with enhanced processing and storage capabilities. But they suffer from limited bandwidth, reliability, load balancing, latency, and security threats.

The main components of the sensor-cloud architecture which can be attacked are the sensor nodes, the communication medium and the remote cloud architecture. The secure pre-processing is used to perform smart sensing and data processing. The communication channel acts as a bridge between the sensors and the cloud architecture, thereby ensuring secure data communication. The cloud's secure runtime services are provided in the sensor-cloud architecture.

It enables a multi-user on-demand sensory system where computing, sensing, and network resources are shared among multiple users and applications. [12] The security issues are mainly because the masses can access this infrastructure for different purposes. Hence, it has security and privacy issues across the sensor-cloud infrastructure. In order to prevent this,

- Secure the sensor node
- Secure communication or wireless channel
- Secure data collection at the sensor node
- Secure data transmission on the communication or wireless channel
- Secure data at the cloud platform

The sensor-cloud architecture is a complex task as it is a combination of policies, technology, and the people which must be managed altogether to design a secure system. Some of the solutions to secure this are:

- End-to-end Encryption - The intensive tasks such as processing and storage are shifted from centralized to the distributed architecture. It gives rise to many security threats and hence, it is highly desirable to apply end-to-end encryption on the data due to the passage of such data from various geographical locations and servers to servers.
- Secure leverages resources - All resources of the cloud are shared among multiple users due to the multi-tenancy model. Hence, it is necessary first to authenticate the users and then secure the shared resources, that is hypervisor, orchestration and monitoring tools.
- Validation of cloud consumer - One of the challenging issues in these environments is the authentication of genuine and legitimate users from intruders and hackers. In this way, the cloud architecture is protected against various malicious activities by attackers.
- Secure interfaces and APIs - They offer automation, orchestration, and management. It is useful to detect, control, and mitigate security issues by tracking malicious interfaces and APIs.
- Insider attacks - These insiders may be either permanent or contractual employees working for an organization and also former employees who have left the company also pose a serious security threat due to their in-depth knowledge of the business process. These attackers work as an agent for the rival organizations for financial gains.

A Higher-Level Security Scheme for Key Access on Cloud Computing is present. Through this scheme, one can use any public cloud system as a private cloud. We consider the data owner an entity consisting of several organization units. A secure mechanism to access the public cloud from both inside and outside the company's network is provided to the authorized people. The idea of this key access control scheme is based on Shamir's secret sharing algorithm and polynomial interpolation method, and is suitable especially for hierarchical organizational structures as it is flexible and secure and offers a hierarchical key access mechanism. Also only authorized users can access the key by making use of the topological ordering of a directed graph, including self-loop. Main overheads such as public and private storage needs are reduced to a tolerable level, and the key derivation is computationally efficient. This method provides both the private cloud security and the functionality, accessibility, and cost savings of the public cloud. This is very secure as it is resistant to collaboration attacks and provides key indistinguishability security. Since the key does not need to be held anywhere, the problem of a data breach based on key disclosure risk is also eliminated.

Dynamical Propagation Model of Malware for Cloud Computing Security can be presented [8].A virtual machine (VM) is susceptible if it is vulnerable to malware attacks i.e the VM does not have an antivirus software or it has expired. A VM is infected if it has been infected by a malware. It is in protected state if it is immune to malware attack, i.e it has unexpired antivirus software installed. Transfer of malware is possible from infected to susceptible and susceptible to protected but impossible from infected to protected.

By doing model analysis, we can find out the dynamic behaviour of the system i.e we can find the equilibrium, local stability and global stability. From the theorems, graphs and numerical simulations, we can conclude that once malware appears in the cloud, it cannot be fully eliminated but by adjusting the related parameters, the proportion of infected VMs can be reduced to a relatively low level. This also provides directional guidance to curb the spread of malware in the cloud. Controlling the propagation of malware in the cloud, over a long period of time is not feasible. The frequency of migration of VMs from physical machines and the proportion of infected VMs in the cloud are directly proportional. The final level of infection depends on system parameters. But the lack of further research on control strategies limits its practicality to a certain extent. Therefore, a study on specific control strategies and application of deep learning methods to explore the propagation behavior of malware in the cloud is required.

Conclusion

Cloud computing and cyber security play major roles in all wakes of life. As seen above, cloud computing plays a significant role in healthcare. New cloud-based user authentication schemes are used for secure authentication of medical data. We use the Modular Encryption Standard (MES) to prevent security breaches and secure confidential health information. Radiation dose verification problem arises for the tumor patients and the modern medical data processing system constructed by cloud computing technology is used to solve this kind of a problem. To enhance the computational capabilities of mobile devices, a multilevel MCC infrastructure based on the granularity of different cloud resources is designed. It plays a major role in security alone. A virtual machine (VM) is susceptible if it is vulnerable to malware attacks and from the results, we can conclude that once malware appears in the cloud, it will always exist, and it cannot be completely eliminated but by adjusting the related parameters, the proportion of infected VMs can be reduced to a relatively low level. Wireless network is integrated with cloud computing forming a new computing paradigm known as sensor-cloud and prevents the low quality of large amount of raw data present. Cloud forensics is an intelligent evolution of digital forensics that defends against cyber-crimes. The proposed Privacy Violation Detection System (PVDS) is a customized system for privacy detection caused by malware in cloud.

References

1. Cloud Centric Authentication for Wearable Healthcare Monitoring System - Srinivas Jangirala, Ashok Kumar Das, Neeraj Kumar, Joel J. P. C. Rodrigues
2. Enhancing Security of Health Information Using Modular Encryption Standard in Mobile Cloud Computing - Maryam Shabbir, Ayesha Shabbir, Celestine Iwendi, Abdul Rehman Javed, Muhammad Rizwan, Norbert Herencsar, Jerry Chun Wei Lin
3. Scalable and Secure Big Data IoT System Based on Multifactor Authentication and Lightweight Cryptography - Saleh Atiewi, Amer Al Rahayfeh, Muder Almiani, Salman Yussof, Omar Alfandi, Ahed Abugabah, Yaser Jararweh
4. Cipher Block Chaining Support Vector Machine for Secured Decentralized Cloud-Enabled Intelligent IoT Architecture - Debabrata Samanta, Ahmed H. Alahmadi, Karthikeyan M. P, Mohammad Zubair Khan, Amit Banerjee, Goutam Kumar Dalapati, Seeram Ramakrishna
5. Digital Forensics Architecture for Evidence Collection and Provenance Preservation in IaaS Cloud Environment using SDN and Blockchain Technology - Mehran Pourvahab, Gholamhossein Ekbatanifard
6. Class: Cloud Log Assuring Soundness and Secrecy Scheme for Cloud Forensics M A Manazir Ahsan, Ainuddin Wahid Bin Abdul Wahab, Mohd Yamani Idna Bin Idris, Suleman Khan, Eric Bachura, Kim Kwang Raymond Choo
7. Towards Building Forensics Enabled Cloud Through Secure Logging-as-a-Service - Shams Zawoad, Amit Kumar Dutta, Ragib Hasan
8. Dynamical Propagation Model of Malware for Cloud Computing Security - Chenquan Gan, Qingdong Feng, Xulong Zhang, Zufan Zhang, Qingyi Zhu.
9. An overview of Mobile Cloud Computing for Pervasive Healthcare - Xiaoliang Wang, Zhanpeng Jin
10. Cloud Computing Assisted Dose Verification System and Method for Tumor Pain Treatment - Maanak Gupta, Mahmoud Abdelsalam, Sajad Khorsandroo, Sudip Mittal.
11. A Multi-Granularity Forensics and Analysis Method on Privacy Leakage in Cloud Environment – Deqing Zou, Jian Zhao, Weiming Li, Yueming Wu, Weizhong Qiang, Hai Jin, Ye Wu, Yifei Yang
12. Sensor-Cloud Architecture: A Taxonomy of Security Issues in Cloud-Assisted Sensor Networks - Ryan Alturki, Hasan Jumaili Alyamani, Mohammed Abdulaziz Ikram, Md Arafatur Rahman, Mohammad Dahman Alshehri, Fazlullah Khan, Muhammad Haleem.
13. Ontology Based Security Context Reasoning for Power-IoT-Cloud Security Service - Chang Choi, Junho Choi