A Review of Ontological Approach toward Cybersecurity in Cloud Computing

Rajiv kumar, Prof. (Dr.) Tarun Kr. Sharma
Shobhit Institute of Engineering and Technology (Deemed to be University), Meerut
Email Id- Rajiv.kumar@shobhituniversity.ac.in, ajay_rana@amity.edu.in, tarun.sharma@shobhituniversity.ac.in

ABSTRACT: The widespread deployment of the Internet allowed for the construction of cloud computing is an emerging IT delivery paradigm. Despite the fact that cloud computing-based services have grown quickly, their security features are in the early stages of development. In order to maintain cloud computing's security, information about cybersecurity that will be shared inside it. It's important to figure out what's going on and talk about it. We are doing so for this reason. Suggest an ontological approach to cloud-based cybersecurity computing. Based on real cybersecurity activities, we provide an ontology for cybersecurity operational information. Mostly concerned with non-cloud computing to talk about it, we have all of the essential cybersecurity knowledge in cloud computing. Use ontologies in cloud computing. We highlight important developments in cloud computing via the debate, such as well as separating data and assets, and clarifying the cybersecurity information needed by changes such as data provenance and encryption information on energy dependencies

KEYWORDS: cybersecurity, cloud computing, information ex- change, Ontological, Open Grid Forum

1.INTRODUCTION

The state of information technology is rapidly changing. The widespread use of the Internet paved the way for the development of a new IT delivery paradigm known as cloud computing. Although there are many definitions of cloud computing, the National Institute of Standards and Technology (NIST) provides one of the most widely accepted definitions: Cloud computing is a paradigm for providing on-demand network access to a shared pool of customizable computing resources (e.g., networks, servers, storage, applications, and services) that may be quickly provided and released with no administrative effort or service provider involvement. Cloud computing is highly scalable, offers a better user experience, and is defined by new Internet-based economics. Following the introduction of cloud computing, cloud services (also known as cloud computing services) have grown in popularity[1]. Cloud services, such as Amazon Web Services and Google Apps, are available via a web browser or a web service application programming interface (API) and are thought to be easy and cost-effective. As a result, the market for cloud services is quickly expanding in terms of expenditure, with estimates ranging from USD 17 billion in 2009 to USD 44 billion in 2013[2]. IT cloud services are projected to increase from 5% of the overall IT market size in 2009 to 10% in 2013, outpacing conventional IT expenditure over the next several years. Individual cloud service providers, on the other hand, offer services with minimal interoperability. It is essential to develop international standards that enhance application portability and enable resource accommodation across cloud service providers in order to establish and secure interoperability. Reliability in disasters may be greatly enhanced because to these improvements. The service interoperability problems are presently being addressed by major organizations such as the Open Grid Forum (OGF), Distributed Management Task Force (DMTF), and Storage Network Industry Association (SNIA)[3]. Despite the fact that the Cloud Security Alliance (CSA) advocates for security problems and provides some security advice, technical standard-building in cloud computing is still in its early phases of development. Protecting cybersecurity in cloud computing necessitates determining what types of cybersecurity data must be shared. We offer an ontological method for this aim. Based on real cybersecurity operations, mostly focused on non-cloud computing, we create an ontology for cybersecurity operational information. We apply the ontology to cloud computing in order to explain the required cybersecurity information. The ontology depicts a comprehensive view of cybersecurity operations and lists the many types of cybersecurity operational data[4]. We explain cybersecurity information that is newly needed or that has to be modified to fit a cloud computing environment for each of these. For example, we examine what kind of incident log will be needed for cloud computing issue management operations, as well as what type of asset description information would be required for managing IT assets for each user company[5]. We highlight important developments in cloud computing, such as data-asset decoupling, and explain the cybersecurity information required by changes like data provenance and resource dependence information, in this debate. Understanding the requirement for an ontology and how certain security ontologies operate is helpful in building an ontology for cybersecurity operational information[5]. An ontology is a formal definition of a conceptualization, which is a simplified, abstract view of the world that we want to describe for a particular purpose. Ontologies are helpful for facilitating information exchange and repurposing. This reusability method is founded on the premise that information may be shared, repurposed, and extended provided a modeling scheme, i.e., an ontology, is clearly defined and unanimously agreed upon by the parties involved[6]. Security ontology that divided ideas into three categories: security, enterprise, and location. Five ideas are introduced in the security subontology: attribute, threat, rating, control, and vulnerability. A security vulnerability ontology that focuses on software vulnerabilities and described the National Vulnerability Database (NVD). Tsoumas et al. added ontological semantics to the DMTF Common Information Model (CIM) standard in order to use it as a container for IS security-related information, and suggested and specified an ontology of security operation for any information system in OWL.A human-behavioral implications-based information security ontology[7]. Before security measures are implemented, this ontology offers a framework for evaluating the unintended consequences of information security management choices on human behavior. Using OWL a number of ontologies for security annotations of agents and online services. They mostly dealt with knowledge representation and certain reasoning problems in the Semantic Web for trust and security. Although additional ontology works exist, their reusability is restricted or they are still in the early phases of development, as Blanco et al. pointed out in a review of security ontologies. Unlike the previous efforts, our emphasis is on real cybersecurity operations, and we are working to create an ontology of cybersecurity operational data. We built the ontology based on extensive talks with cybersecurity operators for practicality and reusability. The ontology may establish language and offer a structure for sharing and reusing cybersecurity operational data[8].

1.1 Operational information ontology for Cybersecurity:

We provide an ontology of cybersecurity operational information based on extensive conversations with prominent cybersecurity operators. Actual cybersecurity activities in the United States, Japan, and Korea were discussed. Despite the fact that each cybersecurity operator has somewhat distinct operations, we were able to create a generic ontology of cybersecurity operational data. The domains for cybersecurity activities. We identify cyber information provided by entities in each operation domain based on domains and entities, and construct the ontology of security operational information in section.

- *Domains of Cyber security Operation*: In cyber society, the phrase "cybersecurity operation" refers to a variety of security activities. Nonetheless, the emphasis of this article is on the cybersecurity activities that ensure the security of information in cyber societies. The protection of information confidentiality, integrity, and availability is known as information security. It may also refer to the information's responsibility, validity, and trustworthiness. IT Asset Management, Incident Handling, and Knowledge Accumulation are the three areas that make up cybersecurity operations. The IT Wealth Management domain manages cybersecurity activities such as installing, configuring, and maintaining IT assets inside each user organization. The IT asset encompasses both user and provider resources; it comprises not just a user's own IT assets, but also network connection, cloud services, and identity services supplied by third parties. By monitoring computing events, incidents made up of multiple computer events, and attack behaviors induced by the incidents, the Incident Handling domain identifies and reacts to incidents that occur in cyber societies. It precisely monitors computer events and generates an incident report when an anomaly is discovered. It analyzes the event in depth based on the report in order to determine the attack pattern and countermeasures. It may provide alerts and advisories to user organizations based on event analysis, such as early warnings of possible risks. The Information Accumulation domain studies cybersecurity and creates knowledge that may be reused by other companies. It offers standard nomenclature and taxonomy, through which it organizes and collects information, for reusability by those organizations.
- *Entities*: This section specifies organizations required to conduct cybersecurity operations in each domain, based on the cybersecurity operation domains the entities are defined from the perspective of functions; therefore, in the actual world, one instance of an entity may be an instance of another entity. Administrator and IT Infrastructure Provider are the two entities that operate in the IT Asset Management area. The Administrator is in charge of the organisation and has access to information about its own IT assets. Each organization's typical example is the system administrator. Each organization's IT infrastructure, which includes network connection, cloud services such as software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS), and identity, is provided by the IT infrastructure Provider. Its most common examples are Internet Service Providers (ISPs) and Application Service Providers (ASPs). There are two entities that operate in the Incident Handling domain: the Response Team and the Coordinator. The Response Team is a group that monitors and analyzes different types of cyber-incidents, such as unauthorized access, DDoS assaults, and phishing, and compiles incident data. It may take countermeasures based on the information, such as adding phishing site URLs to blacklists. A classic example is the incident response team inside a Managed Security Service Provider (MSSP). The Coordinator is an entity that works with the other organizations to coordinate and handle prospective risks based on previous events and crime data. A prominent example is the CERT Coordination Center (CERT/CC), which may be commercial or non-commercial. The Researcher, Product & Service Provider, and Registrar are the three organizations that operate in the Knowledge Accumulation domain. The Researcher is an entity that conducts cybersecurity research, takes information from it, and stores it. Cybersecurity research teams inside MSSPs, such as IBM's X-force and the Little eArth Corporation Co., Ltd.'s Risk Research Institute of Cyber Space, are prominent examples. The Product & Service Provider is a person or company that has

access to information on goods and services, such as their names, versions, vulnerabilities, fixes, and configuration. Its usual examples are a software firm, ASP, and a single private software programmer. The Registrar is an institution that organizes, classifies, and collects cybersecurity knowledge given by the Researcher and Product & Service Provider so that it may be repurposed by another company. The National Institute of Standards and Technology (NIST) and the Information-Technology Promotion Agency of Japan (IPA) are two examples.

1.2 Cybersecurity Information:

- *Database of Incidents*: The Incident Database is a database that stores information on incidents. Such data is manipulated by the Response Team. The event record, incident record, and assault record are the three main types of data kept in this database. The event record is a log of computer events that contains data about packets, files, and transactions. The majority of data are often given automatically by computers as computer logs; for example, logs such as log-in time and date, as well as terminal information provided when root users log in to a system. One kind of event record is this log. The record may be described using the Common Event Expression (CEE) [9]. The incident record is a log of events that includes descriptions of occurrences such as computer states and their outcomes. This record is generated through automated and/or human assessments of numerous event records and associated conjectures. When excessive access to a computer is discovered, for example, the condition of the computer, i.e. excessive access, as well as the anticipated result, i.e. denial of service, should be documented in an incident record. On the basis of this record, the severity of the event and the necessity for countermeasures may be assessed. It's worth noting that an incident record may include fake events, such as incident candidates that were later determined to be non-incidents following an inquiry. The record may be described using the Incident Object Description and Exchange Format (IODEF) . The attack record is a list of attacks generated from incident log analysis. It details the attack chronology, including how the attack began, which IT assets were targeted, and how the harm from the assault spread.
- *Database of Warnings*: The Warning Database is a database that keeps track of cybersecurity alerts. Such data is manipulated by the Response Team and the Coordinator. The Incident Database and Cyber Risk Knowledge Base are used to generate these alerts. User organizations may take countermeasures for indicated cybersecurity threats based on the warnings.
- *Database of User Resources*: The User Resource Database is a database that collects information on assets within individual organizations, including a list of software/hardware, their configurations, resource usage status, security policies, such as access control policies, security level assessment results, and intranet topology. Such data is manipulated by the Administrator. The Assessment Findings Format (ARF) and Common Result Format (CRF) may be used to summarize the results of an IT asset assessment, while the Common Vulnerability Scoring System (CVSS) Common Weakness Scoring System (CWSS) can be used to evaluate the security level of an IT asset .This database also includes cloud service subscription information that the individual user organization is using, such as a list of subscribing cloud services (e.g., data center and SaaS) and a use record for the services.

- *Database of Provider Resources*: The Provider Resource Database is a collection of data about assets that exist outside of particular companies. The information is manipulated by the IT Infrastructure Provider. External network information and external cloud service information are the database's two major components. information about security operations External network information includes inter-organization network topology, routing information, access control policy, traffic status, and security level for networks with which one organization is linked to other organizations. Each cloud service's external cloud service information contains service specs, workload information, and security policy information. It's worth noting that user-specific information, such as local setup information for each cloud service, is saved. Knowledge Base on Cyber Risks: The Cyber Risk Knowledge Base is made up of two knowledge bases: the Vulnerability Knowledge Base and the Threat Knowledge Base. It collects cybersecurity risk information. The Vulnerability Knowledge Base collects known vulnerability data, such as the name, taxonomy, and enumeration of known software and system vulnerabilities, as well as vulnerabilities induced by misconfiguration. It also contains data on human vulnerabilities, or flaws that are revealed by human IT users. Common Vulnerabilities and Exposures (CVE) and Common Weakness Enumeration (CWE) may be used to characterize the contents of the knowledge base. The Threat Knowledge Base collects information on known cybersecurity threats, such as attack and misuse knowledge. Attack knowledge is information on assaults, such as attack patterns, attack tools (such as malware), and trends. Past attack patterns in terms of location and assault target, for example, as well as statistical information on previous attacks, are examples of trend information. The contents of the knowledge base may be described using CAPEC (Common Attack Pattern Enumeration and Classification) and MAEC (Malware Attribute Enumeration and Characterization). Mis-use knowledge focuses on mis-uses that result from users' improper behavior, which may be both benign and harmful. Mis-typing, mis-recognition due to inattentional blindnes, mis-understanding, and getting trapped in phishing traps are examples of benign use. Compliance violations, such as illegal service use and access to unsuitable content, are examples of malicious usage. The Researcher and Product & Service Provider supply this information, which is then structured and categorized by the Registrar[10].

1.3 Cybersecurity in cloud computing:

- *Database of User Resources*: User resources are those that users may access regardless of where they are physically located, whether on a local IT asset or in the cloud. As a result, cloud service subscriptions may be considered user resources. According to this perspective, the User Resource Database must contain two extra kinds of data for cloud security: cloud service subscription information and resource dependence information. Furthermore, to accommodate cloud computing, security level information such as security level assessment findings should be evaluated. The three problems stated above are addressed in the subsections that follow.
- *Subscription Information for Cloud Services*: The cloud resource list, data access control policy, and identity information are all important parts of Cloud Service Subscription Information. The list of cloud resources to which an organization subscribes, which includes data, apps, hardware, and services, must be kept up to date by an Administrator.

The information in the list may be shared with other internal entities. For example, a system administrator from a company's headquarters must keep track of its branches' compliance. Alternatively, this individual may be required to install the same cloud services across all branches in order to maintain a consistent IT environment and security level. External entities may also be given access to this information. Some goods and/or services, for example, may be set automatically depending on the subscriber list in order to function successfully and efficiently. As previously said, thelist will be shared across various companies, both internal and external, and it is anticipated that computers would manage it automatically. As a result, the list's description format must be standardized in order for it to be machine-readable. User data access privileges, such as reading, writing, and executing, are defined by the data access control policy.

2. DISCUSSION

Based on real cybersecurity operations, mostly focused on non-cloud computing, we created an ontology for cybersecurity operational information. We used the ontology to cloud computing in order to explain the required cybersecurity information. We highlighted three main variables that influence cybersecurity information in cloud computing throughout the discussion: data-asset decoupling, the composition of various resources, and the use of external resources. We identified the cybersecurity information required by key changes such as data provenance and resource dependence information, based on developments in cloud computing. Furthermore, we discovered that the security paradigm is changing, with availability becoming one of the most essential elements. Quality cybersecurity operations in cloud computing will be accomplished, and cybersecurity in cloud computing will be substantially enhanced, by applying the cybersecurity information provided in this article.

3. CONCLUSION

This article suggested an ontological approach to cloud computing cybersecurity. Based on real cybersecurity operations, mostly focused on non-cloud computing, we created an ontology for cybersecurity operational information. We used the ontology to cloud computing in order to explain the required cybersecurity information. We highlighted three main variables that influence cybersecurity information in cloud computing throughout the discussion: data-asset decoupling, the composition of various resources, and the use of external resources. We identified the cybersecurity information required by key changes such as data provenance and resource dependence information, based on developments in cloud computing. Furthermore, we discovered that the security paradigm is changing, with availability becoming one of the most essential elements. Quality cybersecurity operations in cloud computing will be accomplished, and cybersecurity in cloud computing will be substantially enhanced, by applying the cybersecurity information provided in this article.

REFERENCES

[1] B. de Bruin and L. Floridi, “The Ethics of Cloud Computing,” *Sci. Eng. Ethics*, 2017, doi: 10.1007/s11948-016-9759-0.

[2] J. Lee, “A view of cloud computing,” *Int. J. Networked Distrib. Comput.*, 2013, doi: 10.2991/ijndc.2013.1.1.2.

[3] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, and A. Ghalsasi, “Cloud computing - The business perspective,” *Decis. Support Syst.*, 2011, doi: 10.1016/j.dss.2010.12.006.

[4] M. Armbrust, A. Fox, and R. Griffith, “Above the clouds: A Berkeley view of cloud computing,” *Univ. California, Berkeley, Tech. Rep. UCB*, 2009, doi: 10.1145/1721654.1721672.

[5] R. Von Solms and J. Van Niekerk, “From information security to cyber security,” *Comput. Secur.*, 2013, doi: 10.1016/j.cose.2013.04.004.

[6] T. Limba, T. Plėta, K. Agafonov, and M. Damkus, “Cyber security management model for critical infrastructure,” *Entrep. Sustain. Issues*, 2017, doi: 10.9770/jesi.2017.4.4(12).

[7] A. Fielder, E. Panaousis, P. Malacaria, C. Hankin, and F. Smeraldi, “Decision support approaches for cyber security investment,” *Decis. Support Syst.*, 2016, doi: 10.1016/j.dss.2016.02.012.

[8] F. Smith and G. Ingram, “Organising cyber security in Australia and beyond,” *Aust. J. Int. Aff.*, 2017, doi: 10.1080/10357718.2017.1320972.

[9] M. Sonntag, “Cyber security,” 2016, doi: 10.2478/hjbpa-2019-0020.

[10] N. Gcaza, R. Von Solms, M. M. Grobler, and J. J. Van Vuuren, “A general morphological analysis: Delineating a cyber-security culture,” *Inf. Comput. Secur.*, 2017, doi: 10.1108/ICS-12-2015-0046.