Processando o Saber
eISSN 2179-5150
FATEC Praia Grande · fatecpg.edu.br/revista
submetido: Jan/2024 · **aceito**: Mar/2024 · **publicado**: Jun/2024
DOI 10.5281/zenodo.14218899

Fundamentos do sistema de detecção de Intrusão e prevenção em ambientes de nuvem

Fundamentals of intrusion detection and prevention system in cloud environments

Siddharth Singh Monteiro Bora
Associação para o Estudo da Literatura e Meio Ambiente do Brasil (ASLE BRAZIL)
sbora08@gmail.com

RESUMO

O NIST (Instituto Nacional de Parametros e Tecnologia – USA) define a Computação em Nuvem como o acesso de rede a um conjunto compartilhado de recursos de computação, configuráveis, que podem ser rapidamente provisionados e liberados com esforço mínimo de gerenciamento ou por meio da interação do provedor de nuvem. Dentro deste contexto, questões relacionadas a segurança se tornam um dos grandes desafios em todas as redes interligadas. Os *Framework* de segurança dos Ambientes de nuvem podem variar de acordo com a tecnologia utilizada. Dentro das quais, podemos encontrar várias opções para habilitar diversos mecanismos de segurança, que são capazes de controlar, monitotorar e restringir o acesso à rede. Neste artigo faço uma analise acerca das noções fundamentais do Sistema de Deteccção de Intrusão e Prevenção (IDPS) em Ambientes de Nuvem. Aditaremos a pesquisa a nossa metodologia de configuração de um sistema IDPS Snort *Software*.

PALAVRAS-CHAVE: Computação em Nuvem; Virtualização; Redes; IDPS Snort.

ABSTRACT

NIST (National Institute of Standards and Technology - USA) defines Cloud Computing as on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. Within this context, security-related issues become one of the major challenges in all interconnected networks. Security frameworks for cloud environments can vary depending on the technology used. Among them, there are various options to enable different security mechanisms capable of controlling, monitoring, and restricting network access. In this article, I analyze the fundamental concepts of Intrusion Detection and Prevention Systems (IDPS) in Cloud Environments. We will augment the research with our methodology for configuring a Snort Software-based IDPS system.

***KEY-WORDS**: Cloud computing; Virtualization; Networks; IDPS Snort.*

INTRODUÇÃO

A computação em nuvem tem um papel importante nas atividades cotidianas de indivíduos e empresas. As informações que transitam entre estes sistemas precisam estar seguras e disponíveis conforme o surgimento da necessidade. As nuvens podem atender a vários grupos de usuários distintos, de tal modo, vários grupos de consumidores diferentes, que compartilham o mesmo conjunto de recursos de forma individualizada, segregada. As pequenas e médias empresas de hoje estão percebendo que ao utilizar os serviços oferecidos na nuvem, podem ter acesso às melhores tecnologias adequando-se até sua infima necessidade (Wang, 2018). Devido ao crescente interesse das empresas pela Nuvem, suas estruturas e serviços, podemos identificar uma preocupação constante por parte dos profissionais de *cybersecurity* em avaliar tendências e tecnologias em questões relacionadas à segurança.

O Instituto Nacional de Padrões e Tecnologia (NIST) define o Modelo de Nuvem "como acesso de rede sob demanda a um conjunto compartilhado de recursos de computação configuráveis e que podem ser rapidamente provisionados e liberados com esforço mínimo de gerenciamento ou por meio da interação do provedor de nuvem.(p.1, 2020)" Do mesmo modo, define Infraestrutura como Serviço *(IaaS)*, sendo a capacidade fornecida ao usuário da nuvem que provisiona o, armazenamento, processamento, montagem de redes e outros recursos fundamentais para complementar seus sistemas computacionais.

O IDPS (Sistema de Detectação de Intrusão e Prevenção)[1] é o processo de monitorar os eventos que ocorrem em um sistema ou rede de computadores e analisá-los em busca de sinais de possíveis incidentes. Incidentes que podem ir desde violações, ameaças iminentes, até ações que violem as políticas de segurança padrão. O *Snort* é um sistema de detecção e prevenção de intrusão de rede de código aberto (www.snort.org). Ele pode analisar a análise de tráfego em tempo real e o fluxo de dados na rede.

A metodologia de pesquisa adotada neste estudo envolve a análise das noções fundamentais do Sistema de Detecção de Intrusão e Prevenção (IDPS) em Ambientes de Nuvem, com foco específico na configuração do *software* IDPS Snort. Inicialmente, será realizada uma revisão da literatura para compreender os conceitos fundamentais da computação em nuvem, virtualização, redes e segurança cibernética. Em seguida, serão identificadas as principais questões de segurança enfrentadas em ambientes de nuvem, destacando a importância de um IDPS eficaz para mitigar ameaças e proteger os recursos compartilhados.

[1] Em português, o termo "IDPS" pode ser traduzido como "Sistema de Detecção e Prevenção de Intrusões" ou, de forma mais simplificada, como "Sistema de Segurança contra Intrusões". Essas traduções capturam a essência da função do IDPS, que é detectar e prevenir atividades não autorizadas ou maliciosas em sistemas ou redes de computadores.

Para a configuração do sistema IDPS utilizando o *software* Snort, será adotada uma abordagem prática, envolvendo a instalação e configuração adequada do *software* em um ambiente de nuvem simulado. Serão consideradas as melhores práticas de configuração e personalização do Snort para atender às necessidades específicas de segurança do ambiente em questão. Por meio dessa abordagem, espera-se contribuir para o desenvolvimento de estratégias de segurança mais robustas e eficientes para ambientes de computação em nuvem.

1. O SISTEMA IDPS – UM *FRAMEWORK* TEÓRICO

Lawal et al. (2019) entende que o IDPS é um dos elementos que compõem a estratégia de segurança da informação de uma organização e deve ser construído em torno do princípio de defesa em profundidade *(Defense in depth*[2]*)* para apoiar outras medidas de segurança implementadas. Dessa forma, o IDPS desempenha um papel fundamental na detecção de tais atividades. De acordo com o NIST (2020):

"A detecção de intrusão é o processo de monitorar os eventos que ocorrem em um sistema ou rede de computadores e analisá-los em busca de sinais de possíveis incidentes, que são violações ou ameaças iminentes de violação de políticas de segurança de computadores, políticas de uso aceitável ou práticas de segurança padrão (p.2)"

Os incidentes têm muitas causas, como *malware* (por exemplo, *worms*, *spyware*), invasores que obtêm acesso não autorizado a sistemas pela Internet e usuários autorizados de sistemas que fazem uso indevido de seus privilégios ou tentam obter privilégios adicionais para os quais não estão autorizados.

Dentro deste contexto, por sua característica funcional, o IDPS é essencial para uma fortificação geral que é instalada em torno de um sistema ou dispositivo. Ele permite justamente a detecção de pacotes e ataques suspeitos, e toma medidas proativas para impedir ou mitigar possíveis danos. Essa capacidade de análise em tempo real e resposta automatizada torna o IDPS uma peça fundamental na defesa cibernética.

[2] Defense in Depth (DiD) é uma abordagem de segurança da informação na qual uma série de mecanismos e controles de segurança são cuidadosamente colocados em camadas em uma rede de computadores para proteger a confidencialidade, integridade e disponibilidade da rede e dos dados nela contidos. Embora nenhuma mitigação individual possa interromper todas as ameaças cibernéticas, juntas elas fornecem mitigações contra uma ampla variedade de ameaças, ao mesmo tempo em que incorporam redundância no caso de falha de um mecanismo. Quando bem-sucedida, essa abordagem reforça significativamente a segurança da rede contra muitos vetores de ataques.

A arquitetura do serviço de computação em nuvem combina três camadas de forma interdependentes: a de infraestrutura, a plataforma e aplicativo (ou aplicação); cada camada pode sofrer de certas vulnerabilidades que são introduzidas por diferentes erros de programação, de configurações, entre outros fatores. Abaixo detalhamos cada uma:

Infraestrutura: Esta camada refere-se aos componentes físicos e virtuais necessários para suportar a computação em nuvem, incluindo servidores, armazenamento, rede e virtualização. Algumas das vulnerabilidades nessa camada podem incluir falhas de segurança no *hardware*, como servidores mal configurados, falhas de autenticação, ou até mesmo ataques físicos aos data centers que hospedam os serviços de nuvem.

Plataforma: Nesta camada, são fornecidos aos desenvolvedores os recursos necessários para criar e implantar aplicativos na nuvem. Isso inclui *frameworks* de desenvolvimento, bancos de dados, sistemas operacionais e outras ferramentas de suporte. As vulnerabilidades nesta camada podem ser introduzidas por falhas de segurança nos sistemas operacionais, configurações inadequadas de permissões ou acesso, e vulnerabilidades nos frameworks e bibliotecas de *software* utilizados no desenvolvimento de aplicativos.

Aplicativo (Aplicação): Esta camada consiste nos aplicativos que são executados na infraestrutura e na plataforma fornecidas pela nuvem. Vulnerabilidades nesta camada podem incluir falhas de segurança no código do aplicativo, como injeção de SQL, XSS (*Cross-Site Scripting*), falhas de autenticação e autorização, entre outras vulnerabilidades de software.

Ao abordar as vulnerabilidades em cada camada, é necessário reduzir os riscos de segurança e garantir a integridade, confidencialidade e disponibilidade dos dados e serviços na nuvem. Deste modo é essencial que os provedores de serviços de nuvem e os usuários finais implementem práticas de segurança rigorosas em todas as camadas da arquitetura de serviço de computação em nuvem.

Sugerimos a utilização de criptografia robusta, políticas de controle de acesso adequadas, monitoramento contínuo de ameaças e vulnerabilidades, e adoção de boas práticas de desenvolvimento seguro de *software*.

De acordo com Shabtai et al. (2010), o IDPS é uma ferramenta indispensável na defeasa cibernética, que realiza a detecção precoce de atividades maliciosas e possivelmente evita danos mais sérios aos sistemas protegidos para lidar com tráfego de acesso à rede em grande escala e controle administrativo de dados e aplicativos.

De acordo com o NIST 800-94 (2007), os IDPSs são compostos por vários tipos de componentes, incluindo sensores ou agentes, servidores de gerenciamento, servidores de banco de dados de redes de gerenciamento, consoles de usuário e administrador. Os sistemas operacionais e aplicativos de todos os componentes devem ser mantidos totalmente atualizados e todos os componentes IDPS baseados em software devem ser protegidos contra ameaças.

a) **Sensores:** Sensores analisam e monitoram. IDPS monitoram redes, incluindo tecnologias baseadas em rede, sem fio e de análise de comportamento de rede. Um sensor IDPS baseado em rede em *host (máquina ou hospedeiro)* monitora e analisa a atividade da rede em um ou mais segmentos de rede. As placas de interface de rede que realizarão o monitoramento são colocadas em *prevention mode* (modo preventivo), o que significa que aceitarão todos os pacotes de entrada que virem, independentemente de seus destinos pretendidos.

b) **Servidor de Gerenciamento***:* Um servidor de gerenciamento é um dispositivo centralizado que recebe informações dos sensores ou agentes e os gerencia. Alguns servidores de gerenciamento executam a análise e a correlação das informações de eventos coletadas que os sensores ou agentes fornecem.

c) **Servidor de banco de dados***:* Um servidor de banco de dados é um repositório de informações de eventos registradas por sensores, agentes e/ou servidores de gerenciamento.

d) **Console***:* os consoles desempenham um papel crucial na administração e monitoramento dos sensores e agentes do IDPS. Um console é um programa que fornece uma interface para os usuários e administradores do IDPS, permitindo a configuração de sensores ou agentes, aplicação de atualizações de *software* e monitoramento e análise das atividades de segurança.

De acordo com Lawal et al. (2019), os sensores e agentes IDPS podem ser implantados de forma independente e gerenciados diretamente por administradores sem a necessidade de um servidor de gerenciamento centralizado.

a) **Baseado em *host***: Os agentes IDPS baseados em host são mais comumente implantados em hosts críticos, como servidores voltados para a Internet, servidores contendo informações confidenciais e dispositivos de usuários finais. Os baseados em host fornecem uma camada adicional de proteção que pode ser usada em combinação para complementar outros sistemas ou controles de intrusão, dependendo dos negócios e dos requisitos de segurança da agência. É importante lembrar que as soluções baseadas em host só inspecionarão o tráfego de ou para o host monitorado, incluindo as atividades do sistema.

b) **Sem fio**: que monitora o tráfego da rede sem fio e o analisa para identificar atividades suspeitas envolvendo os próprios protocolos de rede sem fio.

c) **Análise de comportamento de rede (NBA)**: que examina o tráfego de rede para identificar ameaças que geram fluxos de tráfego incomuns, como ataques distribuídos de negação de serviço (DDoS), certas formas de *malware* e violações de políticas (por exemplo, um sistema cliente que fornece serviços de rede para outros sistemas).

d) **Sensores Baseados em rede**: Os sensores baseados em rede são utilizados para o monitoramento de segmentos específicos ou porções maiores de uma rede, em oposição à implantação de sensores de host (dependendo dos requisitos). Arquiteturas de rede; os componentes do IDPS podem ser conectados uns aos outros por meio de redes padrão de uma organização ou por meio de uma rede separada estritamente projetada para gerenciamento de software de segurança conhecida como rede de gerenciamento (NIST, 2007). Os sensores de rede podem ser implantados nos seguintes modos:

d.1) **Sensores *inline***: A implantação de sensores IDPS *inline* é permitir que eles interrompam ataques bloqueando o tráfego de rede. Os sensores em linha são normalmente colocados em local em que os *firewalls* de rede e outros dispositivos de segurança de rede seriam colocados - nas divisões entre redes, como conexões com redes externas e fronteiras entre diferentes redes internas que devem ser segregadas. O objetivo de implantar sensores em linha é negar que ataques detectados ocorram ou executem outra ação predefinida. Os

sensores IPS são normalmente implementados no ambiente de perímetro do *gateway* ou entre redes internas.

d.2) **Sensores passivos**: Os sensores passivos são normalmente implantados para que possam monitorar os principais locais de rede, como as divisões entre redes, e os principais segmentos de rede, como a atividade em uma sub-rede de zona desmilitarizada (DMZ). Nesses casos, nenhum tráfego realmente passa pelo sensor. Portanto, é possível realizar uma análise mais detalhada, uma vez que não é feita em tempo real. Os sensores passivos geralmente são implantados para que possam monitorar segmentos de rede específicos, o que é mais econômico. Os sensores passivos podem monitorar o tráfego integrando-se à infraestrutura existente, por meio de portas *span* ou *taps* de rede.

2. MODOS OU ESTADOS DE DETECÇÃO

Os modos ou estados de detecção são diferentes abordagens ou métodos utilizados por um Sistema de Detecção e Prevenção de Intrusões (IDPS) para identificar atividades suspeitas ou maliciosas em uma rede ou sistema. Esses modos geralmente se dividem em duas categorias principais: detecção baseada em assinatura e detecção baseada em anomalias.

a) **Baseada em Assinatura**: Segundo o NIST (2007), a detecção baseada em assinatura é altamente eficaz na identificação de ameaças conhecidas, mas inadequada para detectar ameaças previamente desconhecidas, aquelas disfarçadas por técnicas de evasão e várias variantes de ameaças conhecidas. Esse método é simples, pois compara a atividade atual, como um pacote ou entrada de log, com uma lista de assinaturas usando operações de comparação de strings. As tecnologias de detecção baseadas em assinatura têm limitada compreensão de muitos protocolos de rede ou aplicativos e não conseguem analisar adequadamente o contexto das comunicações complexas.

b) **Baseado em Anomalias**: A detecção baseada em anomalias compara definições do que é considerado atividade normal com eventos observados para identificar desvios significativos. Um IDPS que utiliza essa técnica possui perfis representando o comportamento normal de usuários, hosts, conexões de rede ou

aplicativos. Esses perfis são desenvolvidos ao monitorar características de atividade típica ao longo do tempo e, em seguida, são comparados estatisticamente com as características da atividade atual para detectar anomalias. Por exemplo, se uma atividade da Web consumir significativamente mais largura de banda do que o normal, o IDPS alertará um administrador sobre a anomalia. Essa abordagem é eficaz na detecção de ameaças desconhecidas, pois não depende de assinaturas específicas.

c) **Análise de Protocolo com Estado**: Na análise de protocolo com estado, o termo "estado" refere-se à capacidade do IDPS de compreender e acompanhar o estado dos protocolos de rede, transporte e aplicativos que possuem uma noção de estado. Isso permite uma análise mais profunda e contextualizada da atividade da rede, o que pode melhorar a detecção de ameaças e reduzir falsos positivos.

3. DISCUSSÃO E RESULTADOS: IMPLANTANDO O SNORT EM UM ABIENTE DE NUVEM

De acordo com Winkler (2017), muitos consumidores atualmente escolhem utilizar serviços de nuvem gerenciados, oferecidos por provedores de serviços designados. Esses serviços podem ser fornecidos em um ambiente operacional de locatário único (dedicado) ou multilocatário (compartilhado), onde os recursos são divididos entre vários usuários. No modelo multilocatário, todos os benefícios, funcionalidades, elasticidade e responsabilidades são assumidos pelo provedor de serviços. Nesse contexto, Winkler destaca que existem diferentes modelos de compromissos entre os diversos tipos de serviços em nuvem.

Além disso, a segurança é uma preocupação essencial ao adotar serviços em nuvem. É aqui que ferramentas como o Snort entram em jogo. O Snort é um sistema de detecção e prevenção de intrusão de rede de código aberto (www.snort.org), capaz de analisar o tráfego em tempo real e identificar diversos tipos de ataques. Ele verifica os pacotes de dados em relação às regras estabelecidas pelo usuário, proporcionando uma camada adicional de segurança para os dados armazenados na nuvem. Portanto, ao implementar serviços em nuvem, é crucial considerar a segurança da rede e a utilização de ferramentas como o Snort para proteger os dados dos usuários

Nos usaremos SNORT para analisar o tráfego em tempo real, ou seja, sempre que algum pacote entra na rede o snort verifica o comportamento da rede.

3.1 *FRAMEWORK SNORT* (ARQUITETURA *SNORT)*

a) **Decodificador de pacotes**: coleta o pacote das interfaces de rede e o envia para ser pré-processado ou enviado ao mecanismo de detecção.

b) **Pré-processador**: Eles trabalham com o snort para modificar, ou organizar, os pacotes antes do mecanismo de detecção para aplicar alguma operação no pacote se o pacote estiver corrompido. Ele corresponde à string inteira e a reorganiza para que o IDS possa detectar a string.

c) **Mecanismo de detecção**: A principal tarefa do mecanismo de detecção é descobrir a atividade de intrusão. Sempre que o mecanismo de detecção encontra no pacote, ele pode gerar um alerta ou usado para registrar o arquivo.

d) **Módulos de saída**: Sempre que o sistema de registro e alerta do Snort gera alerta e arquivo de registro, os módulos de saída salvam essa saída e também controlam a saída diferente devido ao sistema de registro e alerta.

A posição estratégica dos sensores é de suma importância em segurança cibernética, sendo referida como Posicionamento Estratégico de Sensores IDPS. As organizações devem sempre considerar o uso de redes de gerenciamento em suas implantações de IDPS baseadas em rede.

De acordo com Lawal et al. (2019), se um IDPS for implantado sem uma rede de gerenciamento separada, deve se considerar ao invés sera necessario uma VLAN para proteger as comunicações IDPS. Além do mais deve-se escolher a rede apropriada para os componentes, os administradores também precisam decidir onde os sensores IDPS devem ser localizados.

4. ESTABELECENDO UMA ESTRATÉGIA DE DEFESA IDPS COM SNORT

Para iniciar o Snort, um usuário deve ter, primeiramente a disposição um sistema operacional *Ubuntu Linux* no *Oracle VM Virtual box*. De tal modo que com isso, na tela de abertura, deve se abrir o terminal, digitando o comando "ifconfig". As informações exibidas devem nos fornecer a *NIC* (Cartão de Interface de Rede) e outras informações relevantes, como o endereço IP(Protocolo de Internet).

Na configuração principal, usamos o comando *sudo gedit /etc/snort/snort.conf* para validar na estrutura de configuração estática do arquivo de configuração do *Snort*. O sistema solicitará a senha do *sudo admin.*

Devemos salientar que o *Snort* possui uma estrutura de arquivos baseado em segmentos específicos, como, variáveis de rede; configuração de decodificadores; mecanismo de detecção de base e etc. E através dele o usuário poderá realizar configurações especificas para operacionalizar.

Focando nas regras locais do sistema ($RULE_PATH), podemos configurar a a "lista negra" (*Blacklist*) impedindo assim que conexões indesejadas com *botnets*, invasores, fontes de spam e outros ataques maliciosos. Um ultima observação é que podemos configurar e habilitar o *SouceFire VRT*. *Sourcefire* é um pertence ao fabricante *Cisco* e auxilia no combate as ameaçãs de redes.

Para ativar o *SNORT*, utilizando o *sudo snort -A console -q -u snort -g snort -c /etc/snort.conf -I "NIC"* . Após executar este comando, o Snort estará ativo e começará a monitorar o tráfego de rede de acordo com as configurações especificadas no arquivo /etc/snort.conf. Qualquer atividade suspeita ou maliciosa detectada será registrada e exibida no console em tempo real, permitindo uma resposta rápida por parte dos administradores de sistema.

4. CONSIDERAÇÕES FINAIS

Devido aos cenários complexos de configuração os ambientes de nuvem se tornarem alvos atraentes para ataques cibernéticos, dentro desse cenário, os sistemas tradicionais de detecção e prevenção de intrusão (IDPS) enfrentam desafios importantes ao tentar serem implementados de forma eficaz, devido à dinâmica e particularidade desses ambientes.

Ao demonstrar a valiosa contribuição do IDPS como uma ferramenta inestimável, evidenciamos sua capacidade de realizar a detecção precoce de atividades maliciosas, potencialmente evitando danos graves aos sistemas protegidos. Essa capacidade torna-se ainda mais crucial diante do cenário de tráfego de acesso à rede em grande escala e do controle administrativo de dados e aplicativos que caracterizam os ambientes de computação em nuvem.

Ademais, é imperativo que os administradores de sistemas mantenham a segurança dos componentes do IDPS de forma contínua. Isso inclui a verificação constante do funcionamento adequado dos componentes, o monitoramento diligente em busca de possíveis problemas de segurança e a realização periódica de backups das configurações.

Essas medidas preventivas visam garantir a integridade e a eficácia do IDPS, especialmente ao aplicar atualizações, evitando a perda inadvertida de configurações essenciais. Assim, ao adotar uma abordagem proativa e diligente na gestão da segurança, os administradores podem fortalecer a resiliência dos sistemas em ambientes de computação em nuvem frente às ameaças cibernéticas em constante evolução.

REFERÊNCIAS

ALMORSY, L., M.; GRUNDY, J.; MULLER, I. (2010). **An Analysis of The Cloud Computing Security Problem Computer Science & Software Engineering**. In Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 30th Nov 2010. Faculty of Information & Communication Technologies Swinburne University of Technology, Hawthorn, Victoria, Australia.

CARVALHO, C.; ANDRADE, R.; COUTINHO, E. ; CASTRO, M.; AGOULMINE, N. (2017). **State of the art and challenges of security SLA for cloud computing**. Computers and Electrical Engineering 1–12. http://dx.doi.org/10.1016/j.compeleceng.2016.12.03.

CLOUD SECURITY ALLIANCE (CSA). (2017). **Top Threats to Cloud Computing. Cloud Security Alliance** - http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.

IQBAL, S.; KIAH M., DHAGHIGHI D.; HUSSAIN, M.; KHAN, S: KURRAM KHAN; CHOO, R. (2018). **On Cloud Security Attacks: A Taxonomy and Intrusion Detection and Prevention as a Service**. Journal of Network and Computer Applications, http://dx.doi.org/10.1016/j.jnca.2016.08.016.

KULDEEP, T.; TYAGI S.; AGRAWAL, R. (2017). **Overview - Snort Intrusion Detection System in Cloud Environment**. International Journal of Information and Computation Technology. ISSN 0974-2239 Volume 4, Number 3 pp. 329-334 International Research Publications House http://www. irphouse.com /ijict.htm.

LAWAL, B.O.; IBITOLA, A.; LONGE, O. (2019). **Strategic Sensor Placement for Intrusion Detection in Network-Base IDS**. Olabisi Onabanjo University Consult Ibadan Centre, Ibadan, Nigeria.

NIST. (2020). **Definition of Cloud Computing.** http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

OPENSTACK. (2020). **Install Guide. OpenStack contributors**. Available at: https://docs.openstack.org//install-guide/InstallGuide.pdf Oct 13.

SILKARI, S. (2020). **A Survey Over the Various Malware Detection Techniques used in Cloud Computing.** Department of CSE (UIT) RGPV Bhopal, India.

SNORT. (2022). **User's Manual. The Snort Project. version 2.9.16**. Available at https://snort-org site.s3.amazonaws.com/production/document_files/files/000/000/249/original/sort_manual.pdf.

VEERAMACHANENI, V.K. (2015). **Security Issues and Countermeasures in Cloud Computing Environment**. International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 4, Issue 5.

WANG, H. (2018). **Survey on Performance Analysis of Virtualized Systems.** George Mason University, 2018.

WINKLER, V. (2017). **Securing the Cloud: Cloud Computer Security Techniques and Tactics by Graham Speake, Vic (J.R.)** Winkler. Syngress publications.