Contents lists available at Science-Gate

International Journal of Advanced and Applied Sciences

Journal homepage: http://www.science-gate.com/IJAAS.html

A hybrid model for detecting and preventing attacks on cloud computing systems using blockchain technology

Ali Aqarni *

Department of Computer Science, College of Computing and Information Technology, University of Bisha, P.O. Box 67714, Bisha, Saudi Arabia

ARTICLE INFO

Article history:
Received 31 October 2024
Received in revised form
28 March 2025
Accepted 17 April 2025

Keywords:
Cloud security
Intrusion detection
Intrusion prevention
Blockchain technology
Hybrid model

ABSTRACT

Cloud computing is increasingly used for processing large volumes of data, particularly in businesses, but concerns about cloud security may hinder its broader adoption. Ensuring data confidentiality and protecting resources are critical aspects of cloud security. Numerous models, frameworks, techniques, and mechanisms have been proposed to detect and prevent attacks on cloud computing systems, mostly focusing on intrusion detection systems (IDSs) and intrusion prevention systems (IPSs). However, traditional IDSs and IPSs are inadequate for detecting and preventing various types of attacks on cloud systems. This study aims to review and analyze existing IDSs and IPSs for cloud computing systems and develop a novel model called the Hybrid Detecting and Preventing Model for Cloud Computing Systems (HDPMCC) using blockchain technology. Employing the design science method, the findings reveal that current IDSs and IPSs mainly address Distributed Denial-of-Service (DDOS) attacks. The proposed HDPMCC comprises five essential components: intrusion detection systems, behavioral analysis, blockchain technology, smart contracts, and privacy-enhancing technologies. Compared to existing IDSs and IPSs, HDPMCC offers a more effective approach for detecting and preventing attacks on cloud computing systems.

1. Introduction

The introduction of cloud computing has significantly transformed the way data is managed and stored. Today, both individuals and businesses can access and use computing resources without physically owning them, and with little time required for setup. Although cloud computing was initially viewed as less secure than traditional computing methods, it has recently become widely accepted by businesses. According to a recent survey by Clutch, 70 percent of business organizations are willing to adopt cloud computing for their processing and storage needs if additional security measures can be implemented (Alam et al., 2019). To protect their networks, IT companies are currently relying on message encryptions and firewalls; however, these cannot be the only means of securing their systems in the future (Bokhari et al., 2014).

Originally, the intrusion detection system (IDS) and intrusion prevention system (IPS) were designed to fill a security gap in most firewalls (Ashoor and Gore, 2011). In general, an IDS consists of software or an appliance that can detect threats such as unauthorized network traffic or malicious attacks. IDSs use predefined rules to identify vulnerabilities in endpoint configurations and determine if they are vulnerable to attack (this is called host-based IDS). In addition, network-based IDS can record activities across a network and then compare them with known attack patterns. On the other hand, an IPS detects packets that contain malicious code, botnets, viruses, and targeted attacks. It can prevent any damage to the network caused by those network activities. Assuming that attackers are mainly interested in getting personal information from customers, such as employee information and financial records, their primary motive is to steal sensitive data or intellectual property. The following are various types of attacks that can negatively affect the confidentiality, integrity, and availability of cloud computing systems:

1. Flooding Attack: It is a type of denial-of-service attack in which the fake packages are flooded by

* Corresponding Author.
Email Address: aqrni@ub.edu.sa
https://doi.org/10.21833/ijaas.2025.04.010
Corresponding author's ORCID profile:
https://orcid.org/0009-0004-0830-8787

the flooder node to consume the network bandwidth and cause the network to become overburdened (Mankotia et al., 2023).
2. Insider Attack: A sophisticated insider attack can be described as an attack committed by a member of the organization, whether they are a current or former employee or a business associate, who maliciously conducts the attack (Rajamanickam et al., 2019).
3. User-to-Root Attack: This refers to a type of attack that involves an attacker initiating the attack with a moderate user account on the system and then extending the weakness to increase root access to the system by using a vulnerability that grows from one user account to another (Kavitha and Preetha, 2019). In this scenario, the attacker has access to a normal user account on the computer and can exploit some vulnerability to gain root access.
4. Cross-Site Scripting (XSS) Attack: It is a type of injection in which a malicious script is used to inject itself into a benign and trusted website to perform malicious activities. The attacker uses a web application to send malicious code, usually in the form of a browser-side script, to a different end-user.
5. Data Breaches Attack: Data breaches are security incidents where unauthorized parties enter sensitive or confidential information, including personal information (e.g., SSNs, bank account numbers, and healthcare data), and corporate data (e.g., customer records and intellectual property) without the permission of the owner.
6. Password Attack: It is one of the most common forms of corporate and personal data breaches that occur during a business day. Password attacks are simply a form of cyberattack where hackers attempt to steal users' passwords.
7. Zero-Day Exploits Attack: A zero-day vulnerability (also known as a 0-day) appears in a piece of software or hardware that is unknown to the vendor and for which no patch or other fix is available. Since the vendor already disclosed the vulnerability or found a way to exploit it, it has zero days to prepare a patch. This attack is also referred to as a zero-day flaw.

In cloud computing systems, traditional IDSs and IPSs are not capable of preventing and detecting the different kinds of attacks that are occurring, which makes them insufficient to monitor and prevent. Accordingly, two objectives were set for this study: 1) to collect and analyze the traditional IDSs and IPSs for cloud computing systems, and 2) to develop a hybrid detection and prevention model for cloud computing systems using blockchain technology by answering the following questions:

1. What are the existing challenges of cloud computing?
2. What are the current detection and prevention techniques/mechanisms for the cloud computing system?

This study contributes to the development of a hybrid model that can detect and prevent different types of cyberattacks targeting cloud computing systems. This model offers a comprehensive approach to safeguarding cloud environments by combining advanced threat detection, intrusion detection, and prevention systems, data encryption, multifactor authentication, confidentiality protection, network segmentation, regular vulnerability assessment, and patch management. The hybrid nature of the model offers enhanced accuracy, early warning, reduced false positives, continuous monitoring, and scalability.

The rest of the paper is organized as follows: the related works is reviewed in Section 2, along with the problem statement and objective. Then, the methodology is explained in Section 3. Afterward, the results and discussion are presented in Section 4. Finally, Section 5 concludes the study and recommends directions for future research.

2. Related works

With the advent of cloud computing, some new security challenges have arisen, which are not present in conventional computing paradigms. There are two types of security concerns: cyber and physical. In physical security, the system's hardware is protected. When a provider infrastructure owns a data center, it must provide preventive security measures such as incombustibility, continuous electric supply, and safety measures against common catastrophes such as floods, fires, and earthquakes (Singh and Chatterjee, 2017). It is important to take cybersecurity measures to protect cloud computing systems from cyber-attacks (Samad et al., 2017).

Several papers have been published in the literature to detect and prevent attacks on cloud computing. For example, in Charhi et al. (2016), a detection approach was proposed based on the risk assessment analysis of attack patterns, requiring the participation of cloud providers and data owners. As an example, an attack would be detected as malicious by both services despite having different impacts.

Several security challenges related to cloud computing were presented by Alam et al. (2019). They summarized the challenges related to IDPS in cloud computing, as well as the solutions available to overcome these issues. Privacy and trust issues can be resolved by this method. According to (Nsabimana et al., 2020), DDOS/DOS attacks can be prevented with a cloud-based Hybrid Intrusion Detection and Prevention System based on signature-based methods and genetic algorithms, which are intended to protect cloud services and resources from CIA (Confidentiality, Integrity, and Availability). To detect and prevent DDOS/DOS attacks using Splunk's web framework (a tool for visualization), they combined Snort-IDS with this framework.

Alqahtani et al. (2014) proposed a new IPS service that prevents SQL injections on cloud

computing websites by using signature-based devices instead of detecting fake signatures. Three virtual machines were used to implement a model.

Based on their origin and categories, Saad et al. (2012) classified specific and traditional attacks on cloud computing. A few existing cloud computing-based IDSs were presented, along with their strengths and weaknesses. Rani (2021) discussed attacks on cloud environments as part of their research. In addition to intrusion detection, intrusion prevention, and hybrid approaches, this paper focuses on intrusion prevention as well. Ficco (2013) proposed a hybrid and event correlation approach for detecting intrusions in cloud computing based on a correlation between events. The method involves collecting diverse information from several cloud levels to identify intrusion symptoms that can be analyzed using ontology to reflect complex event patterns. In Sharma et al. (2020), three ML algorithms (J48, Naive Bayes, and oneR) were proposed to identify and prevent attacks based on machine learning. The J48 algorithm exhibited the highest classification performance among all (achieving an accuracy of 94.5% and a sensitivity of 94%). The problem with this approach is that it is meant only to combat web-based attacks.

Bahassi et al. (2022) conducted a literature review on how machine learning has been used to mitigate cybersecurity attacks over the last few years, because of the rapid growth in machine learning in the field of cybersecurity. Accordingly, this work presents promising perspectives for improving cybersecurity through machine learning algorithms in the future.

Furthermore, several digital forensics initiatives have been put forward to detect and analyze the threats and risks that organizations encounter. Employing digital forensics can serve as a highly effective tool for organizations to identify potential security threats and incidents, alleviate risks, and enhance their overall security stance by leveraging digital forensics to minimize vulnerabilities. Many contributions have been proposed and developed by the authors in this area (Kebande and Ray, 2016; Kebande and Venter, 2016; Abd Razak et al., 2016; Kebande et al., 2020; Saleh et al., 2021; 2023; Alhussan et al., 2022; Alshammari, 2023; Salem et al., 2023; Ullah et al., 2023) to examine and identify cybercrime, data breaches, and other digital risks to organizations.

2.1. Problem statement

Cloud security needs to ensure data security and resource protection. For detecting and preventing attacks on cloud computing systems, a variety of models, frameworks, techniques, approaches, and mechanisms have been proposed over the last few years. There have been several studies conducted on IDSs and IPSs over the last few years. As a result, traditional IDSs and IPSs are insufficient to detect and prevent various types of attacks against cloud computing systems.

2.2. Objectives of the study

During this study, two objectives were aimed: first, to collect and analyze each of the traditional IDS and IPS for cloud computing systems, as well as second, to develop a novel hybrid detecting and preventing model for cloud computing systems (HDPMCC) based on blockchain technology.

3. Methodology

This study utilizes design science research methodology (DSRM) to develop detection and prevention models for cloud computing systems. DSRM is defined as a methodology aimed at developing and validating prescriptive knowledge that can be applied to various problem settings. (Peffers et al., 2007) emphasized the difference between the natural sciences, which explain how things are, and the design sciences, which determine what should be and how it should be done. In other words, design science is concerned with designing artifacts to reach a certain goal. DSRM is a label that refers to a set of research methods associated with the design science paradigm. As a result, it encompasses a wide range of methodologies from several disciplines, including information technology, with specific guidelines for evaluating and iterating research projects within it. Adaptations of the methodology used for this study were made based on as shown in Fig. 1.

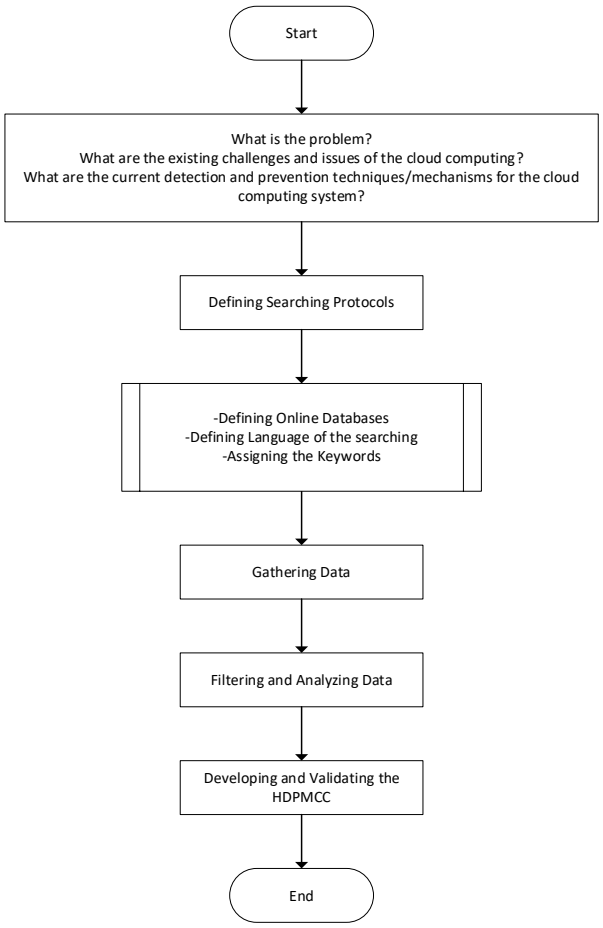

Fig. 1: Adapted methodology (Al-Dhaqm, 2019)

To gather the data from the defined online databases, the author used the protocols defined earlier. Table 1 displays the output of this phase. A total of 3,358 articles were gathered from the five online databases. More specifically, 2,990 articles were gathered from Google Scholar, 202 from Springer Link, 157 from Science Direct, 6 from Scopus, and 3 from Web of Science. These articles were found distributed among book chapters, conference papers, research articles, review articles, and reference work entries. In the next phase, all the captured data were filtered and analysed.

In the filtering and analyzing phase, the author used the inclusion and exclusion criteria to select the relevant articles for this study. In this process, all the book chapters and reference work entries (a total of 238 items) were excluded, whereas all research articles, review articles, and conference articles (a total of 3,075 articles) were included. Then, of those 3,075 articles, the duplicate articles, articles without results, and articles not focused on the subject defined as irrelevant articles were excluded. As a result, 15 articles were selected as the subject of this study, each of which was focused solely on the detection and prevention of attacks on cloud computing systems (Table 2).

After analyzing the 15 articles, the author found that most of the models and techniques of IDS and IPS developed for cloud computing are based on traditional mechanisms, with most of the detection and prevention models focusing on DDoS attacks. Therefore, the author proposes to develop a hybrid detecting and preventing model for cloud computing systems (HDPMCC). This model can detect and prevent attacks on cloud computing systems, using blockchain technology.

To develop the HDPMCC, first, the author extracted the main processes and concepts from the selected 15 models (Table 3). Next, the author selected the common processes and concepts presented in Table 4.

HDPMCC incorporates a combination of traditional security methods and blockchain technology to improve the overall security of cloud systems. This model consists of five main components as shown in Fig. 2:

1. Intrusion Detection Systems (IDSs): In traditional IDS, network traffic is monitored and analyzed to detect anomalous or suspicious activities that may be occurring. A significant part of their role includes identifying potential threats and alerting administrators about the potential threat.
2. Behavioral Analysis: It is used to identify abnormal behavior patterns in the cloud infrastructure because of its use of behavioral analysis techniques. With a model that analyzes user behavior, system activities, and network traffic, the signs of unauthorized access or malicious activities can be detected.
3. Blockchain Technology: Blockchain is a technology that enables transactions to be stored and validated in a decentralized manner. This technology, when applied to cloud systems, can be used to store sensitive information, such as authentication credentials, securely and in an immutable way. This makes it an ideal candidate for use in cloud systems.
4. Smart Contracts: This is a form of self-executing contract, where the terms of an agreement between buyer and seller are directly written into the lines of code, which can then be executed automatically. Smart contracts in cloud systems can be used to automatically enforce security policies and control access to sensitive data as part of security policies. The integration of blockchain technology, particularly through smart contracts, enhances the security framework of cloud computing systems. By automating threat detection and response, enforcing policies, maintaining data integrity, and providing transparency, this hybrid model significantly mitigates the risks associated with cloud services. As threats continue to evolve, the leveraging of blockchain and smart contracts within cloud environments presents a promising approach to bolster security and protect sensitive information.
5. Privacy-Enhanced Technologies: Data security protocols, such as encryption and secure communication protocols, are used to ensure that data is kept confidential while it is in transit and at rest.

4. Results and discussions

This section discusses the advantages and disadvantages of the developed HDPMCC and compares it with the IDSs and IPSs already proposed in the literature. HDPMCC has several advantages: first, it uses both detection and prevention mechanisms to increase accuracy when identifying and mitigating cyber threats.

Table 1: Summarization of the gathering phase

Online database	Articles	Keywords	Year	Language	Content-type				
					Book chapter	Conference paper	Research article	Review article	Reference work entry
Google Scholar	2990	Cloud computing; attack; IDS/IPS	2010-2024	English	90	900	1200	800	0
Springer Link	202	Cloud computing; attack; IDS/IPS	2010-2024	English	148	62	101	7	4
Science Direct	157	Cloud computing; attack; IDS/IPS		English	38	0	78	39	2
Scopus	6	Cloud computing; attack; IDS/IPS	2010-2024	English	1	0	5	0	0
Web of Science	3	Coud computing; attack; IDS/IPS	2010-2024	English	0	0	3	0	0

Table 2: Summarization of the IDS and IPS models focused on cloud computing systems

Reference	Advantages	Disadvantages	The mechanisms used for detecting and preventing	Detected attack types										
				1	2	3	4	5	6	7	8	9	10	11
Charhi et al. (2016)	The findings of this study enable organizations to enhance their cybersecurity posture, identify and mitigate cyber threats effectively, and continuously improve their detection and response capabilities.	Engaging cloud providers and data owners in the risk assessment and detection process requires dedicated time and resources.	IDS and IPS	☒	☒	☒	☒	☒	☒	☒	√	☒	☒	√
Alam et al. (2019)	The advantages of this move include the increase in the amount of research efforts, the sharing of knowledge, increasing the opportunities for publication, and advancing technology.	There are a few issues concerning communication and coordination that impede the successful completion of this project, making it difficult to arrive at an understanding of the subject matter holistically and completely.	IDPS tools	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
Nsabimana et al. (2020)	This study offers a more efficient and effective detection system, as well as real-time reactions, flexibility, cost optimization, and a continuous monitoring system.	It is focused on DDOS/DOS attacks.	Hybrid Intrusion Detection and Prevention System based on signature-based methods and Genetic Algorithms	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	√
Alqahtani et al. (2014)	A new IPS service prevents SQL injections on cloud computing websites by using signature-based devices rather than detecting fake signatures. Using three virtual machines, the model was implemented.	There is a limited amount of customization, signature exploits, limited resources, and the possibility of false positives.	Signature-based devices	☒	☒	☒	☒	☒	√	☒	☒	☒	☒	☒
Saad et al. (2012)	It shows that classified specific attacks offer several advantages, such as enhanced focus, due diligence, and compliance.	Nevertheless, they also come with some disadvantages, such as the fact that they are resource-intensive, limited in scope, and potentially damaging in nature.	IDS	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	√
Rani (2021)	Using an intrusion detection and prevention perspective within the cloud offers several advantages, including reducing security costs, improving scalability, being able to detect and respond to intrusions in real time, and leveraging a centralized management system.	There are many disadvantages associated with cloud computing in this study, including data privacy concerns, dependency on cloud service providers, a lack of control, and the complexity of implementation and management.	IDS and IPS	☒	√	☒	☒	√	☒	☒	☒	☒	☒	√
Ficco (2013)	Hybrid systems achieve a higher level of detection effectiveness by combining the advantages of traditional intrusion detection systems and the advantages of event correlation techniques to provide a more comprehensive and effective protection system.	The disadvantages of hybrid systems are that they can be more complex to implement and maintain, and they may also be more likely to produce false positives.	DS and IPS	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	√
Salas (2024)	The authors of the paper have presented an approach to the collection and characterization of traffic in a real broadband access network by using a real-time traffic dataset developed by the authors. According to the proposed characterization, alerts can be classified with a precision of 93% in the detection of legitimate and anomalous flows while being able to reduce by 73% the traffic flowing through the traffic analyzer without compromising the number of alerts sent.	Owing to a lack of availability, privacy and security concerns, data integrity and reliability issues, incomplete coverage, cost considerations, and technical challenges, the collected data may have difficulty being accurate, reliable, and usable.	IDS	√	☒	☒	☒	☒	√	☒	☒	☒	☒	√
Sahi et al. (2017)	An enhanced security system, an early warning system, customizable rules, automated response, and real-time monitoring are some of the benefits of the proposed system for monitoring and classifying packets in a cloud environment.	Complexity, false positives, false negatives, the lack of coverage, concerns about privacy, and costs are further challenging the technology that faces.	Support vector machines based on least squares, naïve Bayes, K-nearest, and multilayer perceptron	√	☒	☒	☒	☒	☒	☒	☒	☒	☒	√
Sharma et al. (2020)	There are several advantages of using J48, Naïve Bayes, and oneR machine learning algorithms to identify and prevent attacks, including their effectiveness, adaptability, real-time detection, and low false positive rate.	The problem with this approach is that it is only meant to be used for web-based attacks.	Naïve Bayes, OneR, Decision table, and Machine Learning classifiers, e.g., J48	☒	☒	☒	☒	☒	√	√	☒	☒	☒	√
Aljuhani (2021)	The objective of this paper is to present a way for preventing, detecting, and mitigating DDoS attacks using Machine Learning algorithms.	Although different algorithms were used in this study, the results of this study show that, despite the use of these algorithms, the accuracy of this study did not exceed 76%.	Machine learning (ML), network functions virtualization (NFV), and software-defined network (SDN).	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	√
Ali et al. (2019)	Based on a combination of ML algorithms, including K-means and K-nearest neighbors, the authors have proposed a framework for detecting DDoS attacks in a software-defined networking environment.	Despite a high classification accuracy of 98%, a high sensitivity of 98%, and a high specificity of 97%, the results presented in this analysis are only suitable for DDoS attacks.	Artificial neural networks	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	√
Karaçay et al. (2020)	This study developed a new protocol that allows the evaluation of detection models so that it can be assumed to be more effective in detecting attacks and protecting against them. It is an approach that provides end-to-end encryption for detection models using lattice-based cryptography to ensure a higher level of security.	However, as this protocol is only intended for IDS users, it cannot be generalized to other types of detection systems.	IDS and IPS	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	√
Khan et al. (2019)	Using distance measurement techniques that possess artificial intelligence properties, it was proposed that an artificial intelligence-based algorithm could be developed for detecting insider attacks on the Internet of Things (IoT).	According to the simulation results used in this study, there was no more than a 50% degree of accuracy.	Artificial intelligence-based algorithm	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	√
Lewandowska (2024)	The researchers evaluated a variety of methods for AI-based feature optimization, as well as machine learning methods, to improve the productivity of both IDSs and IPSs.	These techniques present several challenges, including complexity, cost, and the possibility of attackers exploiting them. To maintain the integrity of our systems and networks, AI-based feature optimization and machine learning algorithms will continue to be evaluated and improved.	IDS and IPS	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	√

1: Flooding attack; 2: Insider attack; 3: User to root (U2R) attack; 4: Phishing and spear-phishing attacks; 5: Man-in-the-middle (MITM) attack; 6: SQL injection attack; 7: Cross-site scripting (XSS) attack; 8: Data breaches attack; 9: Password attack; 10: Zero-day exploits attack; 11: Denial-of-service (DoS) attacks

By providing early detection capabilities, the model enables a timely response to potential threats, which minimizes the impact of cyberattacks and allows users to take a timely response. This model reduces false positives by relying on advanced algorithms to detect threats, resulting in an efficient use of resources due to reducing false positives. In addition to providing continuous defense against evolving cyber threats, the model ensures that cloud environments are constantly monitored and protected, regardless of the time of day. The model has several advantages, including its ability to adapt to growing cloud environments, which makes it effective regardless of the size of the cloud deployment.

HDPMCC can safeguard cloud environments comprehensively through advanced threat detection, intrusion detection, data encryption, multi-factor authentication, confidentiality protection, network segmentation, vulnerability assessments, and patch management. Because of its hybrid nature, the model offers enhanced accuracy, early warning, reduced false positives, continuous monitoring, and scalability, making it a valuable tool in the battle against cyber-attacks.

In comparison with the existing IDSs and IPDs developed for cloud computing systems, HDPMCC is more comprehensive and able to detect and prevent all the existing cyber-attacks, as shown in Table 4.

Table 3: Processes and concepts extracted from the selected IDS/IPS models

Reference	Extracted processes and concepts
Charhi et al. (2016)	Cloud Computing, Risk Assessment, Attack Patterns, False Positive, Intrusion Detection, Implementation of Approach, Cloud Environment, Intrusion Detection System, Risk Assessment Methodology, False Alerts, Ontology, Risk Score, False Alarm, Cloud Data, Data Owner, Attack Success, Attack Scenarios, Cloud Providers, Cloud Layer, Attack Vector
Alam et al. (2019)	Intrusion detection, Cloud computing, Intrusion prevention, IDS, IPS, IDPS, Security
Nsabimana et al., (2020)	Hybrid Intrusion Detection and Prevention System, Genetic Algorithm, DDOS/DOS Attacks, Snort-IDS, Cloud Attacks
Alqahtani et al. (2014)	Cloud computing, databases, servers, intrusion detection, educational institutions
Saad et al. 2012)	Cloud computing, intrusion detection, intrusion prevention, computer attacks, network attacks, cloud security
Rani (2021)	Computer Network Security, Intrusion Detection, Intrusion Prevention, Intrusion Detection and Prevention Systems, Cloud Computing
Ficco (2013)	Computer clouds, intrusion detection systems, security, correlated events, complex event processing
Salas (2024)	Attack Classification Method, Web Facilities, Brute Force, Spoofing, Flooding, Denial-of-Services, Injection
Sahi et al. (2017)	Categorization, cloud computing, DDOS attacks, least squares support vector machine (LS-SVM)
Sharma et al. (2020)	Web-based attacks, detection, machine learning, feature extraction
Aljuhani (2021)	Internet of Things, Network functions Virtualization, Software-Defined Network, DDOS Attacks, Detection, Machine Learning
Ali et al. (2019)	Software Defined Radios, DDOS, Network Security, Avionics Radios Networks, Diverse Wireless Networks
Karaçay et al. (2020)	Cybersecurity, lattice-based homomorphic encryption, machine learning, binary decision tree, intrusion detection systems, privacy-preserving data classification
Khan et al. (2019)	Artificial intelligence, insider attacks, malicious threats
Lewandowska (2024)	Intrusion prevention system, intrusion detection systems, intrusion response system, anomaly, signature, heuristic, network, host, hybrid, cloud

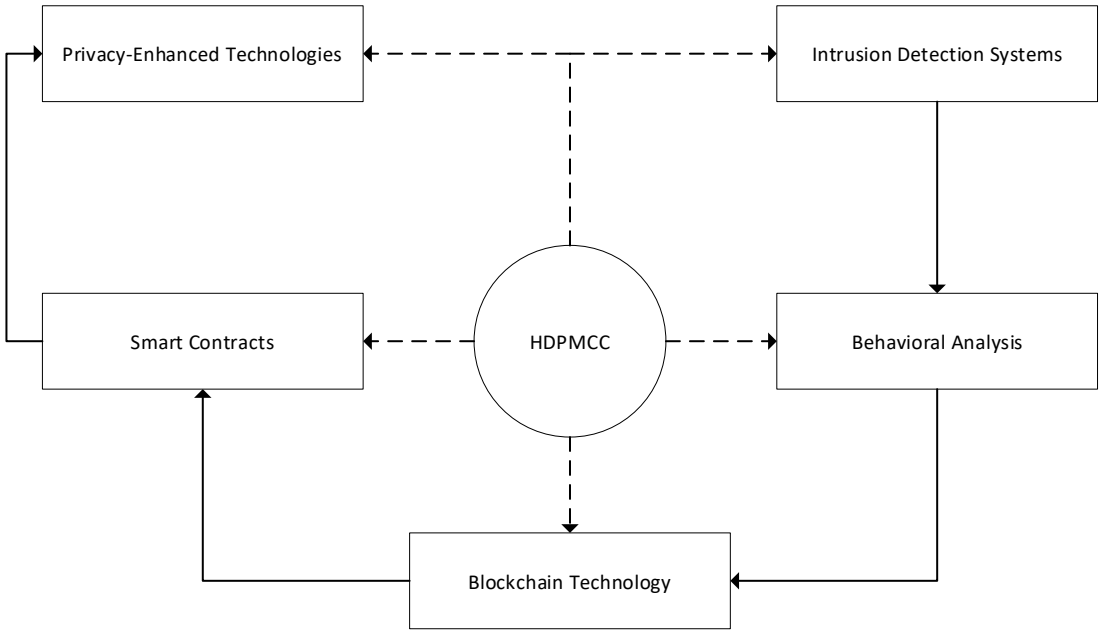

Fig. 2: Structure of HDPMCC

Table 4: Comparison between the developed HDPMCC and the existing IDSs and IPSs

Reference	Detected Attack Types										
	1	2	3	4	5	6	7	8	9	10	11
Charhi et al. (2016)	☒	☒	☒	☒	☒	☒	☒	√	☒	☒	√
Alam et al. (2019)	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
Nsabimana et al. (2020)	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	√
Alqahtani et al. (2014)	☒	☒	☒	☒	☒	√	☒	☒	☒	☒	☒
Saad et al (2012)	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	√
Rani (2021)	☒	√	☒	☒	√	☒	☒	☒	☒	☒	√
Ficco (2013)	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	√
Salas (2024)	√	☒	☒	☒	☒	√	☒	☒	☒	☒	√
Sahi et al. (2017)	√	☒	☒	☒	☒	☒	☒	☒	☒	☒	√
Sharma et al. (2020)	☒	☒	☒	☒	☒	√	√	☒	☒	☒	√
Aljuhani (2021)	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	√
Ali et al. (2019)	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	√
Karaçay et al. (2020)	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	√
Khan et al. (2019)	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	√
Lewandowska (2024)	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	√
The developed HDPCC	√	√	√	√	√	√	√	√	√	√	√

1: Flooding attack; 2: Insider attack; 3: User to root (U2R) attack; 4: Phishing and spear-phishing attacks; 5: Man-in-the-middle (MITM) attack; 6: SQL injection attack; 7: Cross-site scripting (XSS) attack; 8: Data breaches attack; 9: Password attack; 10: Zero-day exploits attack; 11: Denial-of-service (DOS) attacks

There are several limitations associated with the proposed HDPMCC that can be outlined in the following paragraphs:

1. Scalability is a critical challenge for blockchain networks, especially public blockchains. As the number of transactions grows, confirmation times lengthen, which delays incident detection and response.
2. Since blockchains are decentralized, they sometimes consume significant computational resources. Consequently, cloud-based infrastructures become inefficient and unable to scale.
3. Integrating blockchain technology with existing cloud infrastructure can be complex and may require substantial changes to the architectural design, which can incur additional costs and time.

The hybrid model for detecting and preventing attacks in cloud computing systems using blockchain technology has the potential for varied, innovative applications across diverse cloud environments. By enhancing data integrity, automating responses, and fostering trust, this approach can contribute significantly to improving organizational security posture, ensuring compliance, and enabling seamless operations in an increasingly complex digital landscape.

5. Conclusions

A growing number of enterprises use cloud computing to process large amounts of data. This technology is of high popularity, but its widespread adoption may be hindered by cloud security issues. The cloud's security must ensure data confidentiality and resource protection. To detect and prevent cloud computing system attacks, several models, frameworks, techniques, approaches, and mechanisms have been proposed in the literature. IDSs and IPSs are the existing intrusion detection and prevention systems. However, traditional IDSs and IPSs are not sufficient to detect and prevent different kinds of attacks on cloud computing systems. Accordingly, this study accomplished two objectives: 1) collecting and analyzing traditional IDSs and IPSs for cloud computing systems, and 2) developing a hybrid detection and prevention model for cloud computing systems using blockchain technology (HDPMCC). Future research could focus on validating HDPMCC and implementing it in real-world scenarios.

Acknowledgment

The authors are thankful to the Deanship of Graduate Studies and Scientific Research at the University of Bisha for supporting this work through the Fast-Track Research Support Program.

Compliance with ethical standards

Conflict of interest

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

References

Abd Razak S, Othman SH, Aldolah AA, and Ngadi MA (2016). Conceptual investigation process model for managing database forensic investigation knowledge. Research Journal of Applied Sciences, Engineering and Technology, 12(4): 386-394. https://doi.org/10.19026/rjaset.12.2377

Alam S, Shuaib M, and Samad A (2019). A collaborative study of intrusion detection and prevention techniques in cloud computing. In the International Conference on Innovative Computing and Communications: Proceedings of ICICC 2018, Springer Singapore, Delhi, India, 1: 231-240. https://doi.org/10.1007/978-981-13-2324-9_23

Al-Dhaqm AMR (2019). Simplified database forensic investigation using metamodeling approach. Faculty of Computing, Department of Computer Science, Universiti Teknologi Malaysia, Skudai, Malaysia.

Alhussan AA, Al-Dhaqm A, Yafooz WM, Razak SBA, Emara AHM, and Khafaga DS (2022). Towards development of a high

abstract model for drone forensic domain. Electronics, 11(8): 1168. https://doi.org/10.3390/electronics11081168

Ali M, Benamrane F, Luong DK, Hu YF, Li JP, and Abdo K (2019). An AI based approach to secure SDN enabled future avionics communications network against DDoS attacks. In the IEEE/AIAA 38th Digital Avionics Systems Conference, IEEE, San Diego, USA: 1-7. https://doi.org/10.1109/DASC43569.2019.9081639

Aljuhani A (2021). Machine learning approaches for combating distributed denial of service attacks in modern networking environments. IEEE Access, 9: 42236-42264. https://doi.org/10.1109/ACCESS.2021.3062909

Alqahtani SM, Al Balushi M, and John R (2014). An intelligent intrusion prevention system for cloud computing (SIPSCC). In the International Conference on Computational Science and Computational Intelligence, IEEE, Las Vegas, USA, 2: 152-158. https://doi.org/10.1109/CSCI.2014.161

Alshammari A (2023). Detection and investigation model for the hard disk drive attacks using FTK imager. International Journal of Advanced Computer Science and Applications, 14(7): 767-774. https://doi.org/10.14569/IJACSA.2023.0140784

Ashoor AS and Gore S (2011). Difference between intrusion detection system (IDS) and intrusion prevention system (IPS). In the Advances in Network Security and Applications: 4th International Conference, Springer Berlin Heidelberg, Chennai, India, 4: 497-501. https://doi.org/10.1007/978-3-642-22540-6_48

Bahassi H, Edddermoug N, Mansour A, and Mohamed A (2022). Toward an exhaustive review on machine learning for cybersecurity. Procedia Computer Science, 203: 583-587. https://doi.org/10.1016/j.procs.2022.07.083

Bokhari MU, Alam S, and Hasan SH (2014). A detailed analysis of grain family of stream ciphers. International Journal of Computer Network and Information Security, 6(6): 34-40. https://doi.org/10.5815/ijcnis.2014.06.05

Charhi YB, Mannane N, Bendriss E, and Regragui B (2016). Intrusion detection in cloud computing based attacks patterns and risk assessment. In the 3rd International Conference on Systems of Collaboration, IEEE, Casablanca, Morocco: 1-4. https://doi.org/10.1109/SYSCO.2016.7831341

Ficco M (2013). Security event correlation approach for cloud computing. International Journal of High-Performance Computing and Networking 1, 7(3): 173-185. https://doi.org/10.1504/IJHPCN.2013.056525

Karaçay L, Savaş E, and Alptekin H (2020). Intrusion detection over encrypted network data. The Computer Journal, 63(1): 604-619. https://doi.org/10.1093/comjnl/bxz111

Kavitha V and Preetha S (2019). Cyber Security issues and challenges-A review. International Journal of Computer Science and Mobile Computing, 8(11): 1-6.

Kebande VR and Ray I (2016). A generic digital forensic investigation framework for internet of things (IoT). In the IEEE 4th International Conference on Future Internet of Things and Cloud, IEEE, Vienna, Austria: 356-362. https://doi.org/10.1109/FiCloud.2016.57

Kebande VR and Venter H (2016). Requirements for achieving digital forensic readiness in the cloud environment using an NMB solution. In the 11th International Conference on Cyber Warfare and Security, ACPI, Boston, USA: 399-406.

Kebande VR, Ikuesan RA, Karie NM, Alawadi S, Choo KK, and Al-Dhaqm A (2020). Quantifying the need for supervised machine learning in conducting live forensic analysis of emergent configurations (ECO) in IoT environments. Forensic Science International: Reports, 2: 100122. https://doi.org/10.1016/j.fsir.2020.100122

Khan AY, Latif R, Latif S, Tahir S, Batool G, and Saba T (2019). Malicious insider attack detection in IoTs using data analytics. IEEE Access, 8: 11743-11753. https://doi.org/10.1109/ACCESS.2019.2959047

Lewandowska N (2024). Intrusion detection systems: Categories, attack detection and response. https://doi.org/10.20944/preprints202402.0008.v1

Mankotia V, Sunkaria RK, and Gurung S (2023). AFA: Anti-flooding attack scheme against flooding attack in MANET. Wireless Personal Communications, 130(2): 1161-1190. https://doi.org/10.1007/s11277-023-10325-3

Nsabimana T, Bimenyimana CI, Odumuyiwa V, and Hounsou JT (2020). Detection and prevention of criminal attacks in cloud computing using a hybrid intrusion detection systems. In: Ahram T, Karwowski W, Vergnano A, Leali F, and Taiar R (Eds.), Intelligent human systems integration 2020. IHSI 2020. Advances in intelligent systems and computing, vol 1131. Springer, Cham, Switzerland. https://doi.org/10.1007/978-3-030-39512-4_103

Peffers K, Tuunanen T, Rothenberger MA, and Chatterjee S (2007). A design science research methodology for information systems research. Journal of Management Information Systems, 24(3): 45-77. https://doi.org/10.2753/MIS0742-1222240302

Rajamanickam S, Vollala S, Amin R, and Ramasubramanian N (2019). Insider attack protection: Lightweight password-based authentication techniques using ECC. IEEE Systems Journal, 14(2): 1972-1983. https://doi.org/10.1109/JSYST.2019.2933464

Rani S (2021). A perspective for intrusion detection and prevention in cloud environment. International Journal of Advanced Networking and Applications, 12(6): 4770-4775. https://doi.org/10.35444/IJANA.2021.12606

Saad EN, El Mahdi K, and Zbakh M (2012). Cloud computing architectures based IDS. In the IEEE International Conference on Complex Systems, IEEE, Agadir, Morocco: 1-6. https://doi.org/10.1109/ICoCS.2012.6458581 **PMid:22383920 PMCid:PMC3279494**

Sahi A, Lai D, Li Y, and Diykh M (2017). An efficient DDoS TCP flood attack detection and prevention system in a cloud environment. IEEE Access, 5: 6036-6048. https://doi.org/10.1109/ACCESS.2017.2688460

Salas MIP (2024). Attack taxonomy methodology applied to web services. Latin-American Journal of Computing, 11(1): 66-79.

Saleh M, Othman SH, Driss M, Al-dhaqm A, Ali A, Yafooz WM, and Emara AHM (2023). A metamodeling approach for IoT forensic investigation. Electronics, 12(3): 524. https://doi.org/10.3390/electronics12030524

Saleh MA, Othman SH, Al-Dhaqm A, and Al-Khasawneh MA (2021). Common investigation process model for Internet of Things forensics. In the 2nd International Conference on Smart Computing and Electronic Enterprise, IEEE, Cameron Highlands, Malaysia: 84-89. https://doi.org/10.1109/ICSCEE50312.2021.9498045 **PMid:34022883 PMCid:PMC8140497**

Salem M, Othman SH, Al-Dhaqm A, and Ali A (2023). Development of metamodel for information security risk management. In: Yafooz WM, Al-Aqrabi H, Al-Dhaqm A, and Emara A (Eds.), Kids cybersecurity using computational intelligence techniques: 243-253. Springer International Publishing, Cham, Switzerland. https://doi.org/10.1007/978-3-031-21199-7_17

Samad A, Shuaib M, and Beg MR (2017). Monitoring of military base station using flooding and ACO technique: An efficient approach. International Journal of Computer Network and Information Security, 9(12): 36-44. https://doi.org/10.5815/ijcnis.2017.12.05

Sharma S, Zavarsky P, and Butakov S (2020). Machine learning based intrusion detection system for web-based attacks. In the IEEE 6th Intl conference on big data security on cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, and IEEE Intl Conference on Intelligent

Data and Security, IEEE, Baltimore, USA: 227-230. https://doi.org/10.1109/BigDataSecurity-HPSC-IDS49724.2020.00048

Singh A and Chatterjee K (2017). Cloud security issues and challenges: A survey. Journal of Network and Computer Applications, 79: 88-115. https://doi.org/10.1016/j.jnca.2016.11.027

Ullah F, Pun CM, Kaiwartya O, Sadiq AS, Lloret J, and Ali M (2023). HIDE-Healthcare IoT data trust management: Attribute centric intelligent privacy approach. Future Generation Computer Systems, 148: 326-341. https://doi.org/10.1016/j.future.2023.05.008