Cloud of Things (CoTs): Security Threats and Attacks

Sara Mutlaq Almtrafi[1], Bdour Abduallatif Alkhudadi[2]
College of Computers and Information Technology
Taif University

Hatim Alsuwat[3]
Department of Computer Science
College of Computer and Information Systems
Umm Al-Qura University

Emad Alsuwat[4]
College of Computers and Information Technology
Taif University

Summary
Cloud of things (CoTs) is a newer idea which combines cloud computing (CC) with the Internet of Things (IoT). IoT capable of comprehensively producing data, and cloud computing can be presented pathways that allow for the progression towards specific destinations. Integrating these technologies leads to the formation of a separate element referred to as the Cloud of Things (CoTs). It helps implement ideas that make businesses more efficient. This technology is useful for monitoring a device or a machine and managing or connecting them. Since there are a substantial amount of machines that can run the IoT, there is now more data available from the IoT that would have to be stored on a local basis for a provisional period, and this is impossible. CoTs is used to help manage and analyze data to additionally create usable information by permitting and applying the development of advanced technology. However, combining these elements has a few drawbacks in terms of how secure the process is. This investigation aims to recent study literature from the past 3 years that talk about how secure the technology is in terms of protecting by authentication, reliability, availability, confidentiality, and access control. Additionally, this investigation includes a discussion regarding some kinds of potential attacks when using Cloud of Things. It will also cover what the various authors recommend and conclude with as well as how the situation can be approached to prevent an attack.

Key words: Cloud of things (CoTs), Security, Attacks and Protection.

1. Introduction

The elements that the integrated technology share must be explored first when investigating computing. This is especially applicable when comparing CC and IoT, as they are similar in many aspects. Integrating these technologies help with their facilitation and improvement. Together, they contribute to the development of the present industry of internet services [1]. Although both technologies are much different from each other, their attributes are complementary. This means that there is a limit to how capable IoTs are when they would have to store or process data, and even perform in a secure, private and reliable manner. Efficiently overcoming such issues is by integrating cloud computing concepts. Additionally, cloud technology increases user-friendliness at cost-efficient prices. Cloud services also assist with the collection, processing, and publishing of information generated using IoTs' technology. It uses IoTs for the expansion of its limitations and to make newer features available to users [1].
Internet of things (IoTs) technology helps with the simplification of labor. It combines the ubiquity and pervasiveness of computing as well as other technology including machines for communication. It helps with the logical interconnection and interoperation of real and virtual elements using predefined internet infrastructures [2]. The newer waves of communication and its utilities would be dependent on the development of the IoT industry, which is now essential in the lives of any individual [3]. IoT technology helps convert any environment such as a home or a building into a smart one. However, more connections lead to more issues (in terms of the ability to store, process and manage information). However, CC had helped to mitigate such issues with clever integration [3].
Cloud computing (CC) refers to technologies of high versatility that can be applied for a very diverse variety of tasks. Such models are used for the sake of convenience, customization of network-related services, and its features that help with the provisioning of useful elements where the interactions with service providers are minimized. Additionally, it is able to address infrastructures needed by larger user bases with specific needs [4].
Several aspects of both CC and IoTs that complement each other can be observed in Table 1. IoT runs efficiently with the use of storage resources and other facilities made available using CC technology [5].

Manuscript received August 5, 2021
Manuscript revised August 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.8.31

Table 1: Features of IoTs and CCs that complement each other

Item	***IoT***	Cloud Computing
Elements	Real world stuff.	Virtual resources.
Reachability	Bounded	Ubiquitous
Storage	bounded or none	Virtually boundless
Connections	Utilizes the Internet converging points.	Utilizes the Internet to deliver services.
data	It generates big data.	It assists to manage big data.

The handling and management of the data generated by IoTs using CC make them complementary. Such a combination is what can be referred to as CoT [6]. Figure 1 displays examples of how IoTs can be applied when professionally integrated with CCs [7].

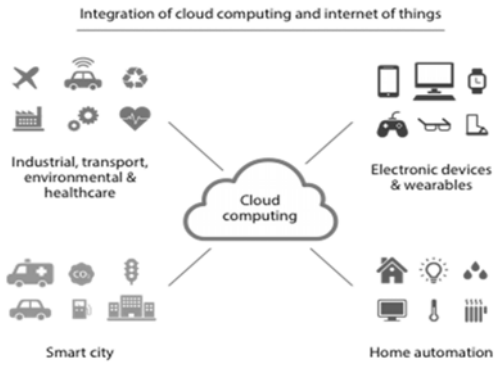

Figure. 1 Convergence of CC and IoT

CoTs consists of virtual elements that can be built atop networks, which assists with efficiency when dealing with data, application, and infrastructure, and is also quite inexpensive. Here, a user can transfer information from physical elements on a global scale through the usage of service-oriented systems. Therefore, it can share any resource that underwent natural distribution with the additional flexibility of the elements within a CC system and interactions with clients [8]. Integration of CC with IoTs can be quite advantageous as a result of:

1. Affordability: Economically, CC solutions are wise due to the lack of required investment to equip infrastructure. It is paid for depending on the demand for a specific resource required by the ISP. This prevents extra fees and the user would only have to spend how much each resource is worth.
2. Flexible: Every aspect including storage and bandwidth is expandable depending on how requested specific services are in the CC industry.
3. Growth Efficiency: The ability to use CC technology anywhere and the removal of physical limitations makes the process more efficient.
4. Security: Storing information in cloud services such as OneDrive is extremely useful in case essential information on a device is lost because the same information can be accessed from other devices, and a remote wipe of the original device can be done if required.
5. Avoidance of delaying and failures: CC connects one server to others, and the failure of one will simply lead to the withdrawal of the loads from the specific nodes to avoid disruptions or delays.
6. Disaster recovery: In case of an emergency that may cause damage to the stored data and other applications, there would usually be severe repercussions due to the loss of information, However, CC technology allows this data to be recovered when required.
7. Compatible to the environment: CC technology does not require energy to run and therefore can be considered to be beneficial to the environment [9].

Large numbers of clients get a chance for active communication and exchanging of any resource or confidential information as a result of this integration, and therefore promising confidentiality would mean taking measures to make sure that the system is secure and private information will not go into the wrong hands [10]. Thus, tools are implemented that externally authenticate information sent or received. Keeping this information secure is quite challenging because ISPs would have the chance of risking reaches or leaks making larger systems quite untrustworthy due to it being easily hackable [11].

This paper will be carried out in 5 parts in which the second will be a summary of recently published literature regarding measures to achieve the security requirements, and the third part will address some kinds of possible threats or attacks and mechanisms for the prevention that objective the CoTs environment. Additionally, there have been several investigations that looked into attacks and measures of prevention. The fourth part of this paper will be a discussion that reviews the steps required to keep the system secure from any attack that was covered in the previous parts of this paper. Finally, the fifth part will be the conclusion of this paper.

2. Security mechanism in cloud of things CoTs

Figure 2. Security Requirements in CoTs

Figure 2. As mentioned above, all the security requirements to ensure that CoTs run in a highly secure manner. This would include the mechanisms that authors implement and address in their literature to achieve this security.

2.1 Confidentiality in CoTs

Understanding if CoTs systems are truly confidential would require us to look into papers written by authors within this discipline. Utilizing the CoTs services requires the sharing of the user's current location. Since this is highly personal, leaking such data [12] would be a huge breach that any user would have to be protected from. For this reason, certain measures are implemented that protect such data. Firstly, there was an analysis of the users' movement patterns using Mobility Markov's chains. They fixed the issue by proposing algorithms that cloaked the location by encompassing a larger area as the location, making it harder to pinpoint an exact location of a user at a given time. Such approaches help protect personal information even if a breach occurs.

Newer measures [13] involved the use of field-programmable gate arrays (FPGA) for the securing of IoT information while it is being processed using CC systems. It can keep this information secret by adding steps to authenticate users using FPGAs which assists with security when implementing symmetric session keys that connect on-cloud FPGAs, IoTs, and their devices, and the clients. It also permits the user to test for configuration integrity as it runs on FPGAs. Symmetric Proxy Re-Encryption (PREs) schemes are utilized for the sake of supporting the published/subscribed to modes in which the IoTs can be operated. The experiment result displays a rate six times greater in the PREs compares to SW implementations when attempting to transform cipher text sized one gigabyte.

The paper [14] includes the proposal for blockchain-aided searchable attribute-based encryptions (BC-SABEs) that efficiently revokes and decrypts in situations in which the conventional centralized servers are substituted using de-centralized blockchain systems that enable a user to use coalition blockchains for the generation of each partial token. CC servers are not solely for storage purposes but can also help with searching and creating pre-descriptions for a user. Tests that analyzed how secure the systems are, help understand how the schemes realize how they must remain secure for chosen plaintext attacks as well as chosen keyword attacks. A simulation displays how decrypting and generating tokens are preferred in terms of costs.

2.2 Authentication and Access Control in CoTs

The proposal for achieving authenticated systems was utilizing two Certificates less Public-key Authenticated Encryption with Keyword Searches (CLPAEKSs). The literature [15] includes an analysis of how secure CLPAEKSs are and displayed that the evidence for CLPAEKS was not correct, which meant that their security was not effective when faced with a keyword guess attack. The paper continued by proposing CLPAEKS that had no channels and provide evidence of security even when faced with a keyword guess attack with the improved security model. This system can be said to be comparably more efficient and more secure.

This literature [16] introduced the proposal of a framework that helps support trusts with IoTs integrated with CC technology. This concerned governmental usage including e-governmental facilities using CoTs. Here, security is ensured by identifying a user or device that has authorization, and they are allowed to utilize CoTs services. There are numerous ways in which such authentications can take place. It was found that the proposal was effective in ensuring environments that can be trusted for CoTs users to utilize the services they require, which even include e-governmental operations.

The literature [17] includes a proposal for the protection of confidential information which involves two steps, of which one involves encrypting this information with the use of RC6, and the second involves encrypting the same with Feistel schemes. Public information that is not confidential undergoes encryption using Advanced Encrypting Standards (AESs). Accessing CoT storage facilities using multi-factor systems to authenticate the same was an additional inclusion in the proposal. When logging in, a user would have to their information which would then be processed by Trusted Authorities (TAs). This proposal must be implemented using the NS3 network simulation. The performances were then observed in terms of duration for computation, encryptions, and decryptions as well as how secure the process was. It was found that the performance was an improvement in comparison with FCSs, CP-ABEs, and MCP-ABEs.

This paper [18] introduces the construction of newer CP-ABE models for the storing and controlling of CoTs data. Attribute authority management (AAMs) modules help to provide access control with ease and also assists with the reduction of public-key overhead storages. An additional proposal was a Secure and Efficient Multi-authority Access Controlling and Storing of the Internet of Things (SEMACSIT) which ensures backward and forward security if specific attributes are no longer applicable to a user. The exploitation of outsourced encrypting simplified key structuring as well as the AAMs, overhead computation faces a drastic decrease. Furthermore, newer User Access Control Lists (UACLs) are built to assist and authorize users of CoTs systems. The study concluded by displaying that there is an observable improvement in how efficient the system is when using SEMACSIT. This happens as a result of decreased overhead computation and highly secure storage systems in comparison with previous models.

The literature [19] analyses each factor that impacts responding durations for the management of permissions using the symmetric and asymmetric signature within a

JSON token. Additionally, computing devices were evaluated experimentally by collecting usage data for the processed and stored information. Mainly, this proposal contributes by focusing on evaluations of trade-offs that involve the safe and strong performance of symmetric HMACs as well as asymmetric RSAs. These contributions focused on selecting and evaluating the quantities in terms of requests and found them to be quite significant. For lower quantities, the performance data for both cryptographies were more or less the same.

2.3 Integrity in CoTs

The paper [20] displays a proposal for a newer idea supporting synchronized updating for numerous data blocks that have high data integrity. SGMHT, which is the extended version of the Merkle Hash Trees (MHTs) based on scapegoats is used. Erasure-coded hierarchies for log structures were additionally employed, supporting late updates to retrieve data and have multiple blocks. Additionally, data transmissions are reduced and the updating process is made efficient with the use of a homomorphic tag in the proposal. The study concluded by displaying the ability of their idea to perform better and more efficiently than any other concept that existed at the time.

The paper [21] discusses a proposal that involves verifying the integrity using ZSS signatures that help to protect personal information and publically audit the same using TPAs. This method is more effective in reducing overhead computation for hash functions in comparison to BLSs. Studies conducted display decreased overhead computation and communications compared to other concepts that were already present. The idea is to support public audits through the introduction of TPAs using random masking techniques for the preservation of personal information. Assuming the CDHs to be difficult, evidence is provided that displays the method's resistance towards adaptive selection attacks using the random oracle models.

2.4 Availability in CoTs

IoTs provide numerous functions that each serve a separate purpose with their features and demand. Thus, optimization occurs very inefficiently within CoTs as the demand cannot be met using the available services. There exists research [22] that attempts to solve this by proposing high availability architecture that can optimize how available specific resources are in a dynamic manner using service characteristics. Verifications of these claims were done by implementing the same on OpenStack, which showed the model's ability to meet the demand through optimized availabilities.

The concepts introduced during this study [23] keeps a record of solely the file content during numerous occasions where snapshots were taken and play no role in the quantity mentioned for each HDFS stored replica. Ideally, there would exist more copied files within each snapshot to make it significantly more available, which in turn provides its enhancements. This, however, cannot be done efficiently. Improvisations and modifications were duly made to HDFSs for the automatic rise in the snapshot replica quantities. Additionally, further improvements can be made to make more copies available to users. The study concluded by displaying the ability of their model to perform better than any other HDFS could at the time in terms of generating more copies to make more available for users.

Table 2: Security Mechanisms in Recent papers to (CoTs)

Ref	***Year***	Security requirements	Mechanism
[12]	2019	Confidentiality	Use Mobility Markov chain
[13]	2018	Confidentiality, Integrity and Authentication	use field programmable gate arrays (FPGAs)
[14]	2020	Confidentiality	Use blockchain-aided searchable attribute-based encryption (BC-SABE)
[15]	2020	Authentication and Confidentiality	Use authenticated encryption (CLPAEKS)
[16]	2019	Authentication and Access control	Use trust framework for government
[17]	2020	Authentication and Confidentiality	Use multifactor authentication and (AES) encryption scheme.
[18]	2020	Access control	Use SEM-ACSIT scheme
[19]	2020	Access control and Authentication	Use symmetric and asymmetric signatures in JSON tokens.
[20]	2020	Integrity	Use balanced data structure SGMHT—an extension of the Merkle Hash Tree (MHT)
[21]	2019	Integrity. Authentication and Confidentiality	Use the ZSS signature algorithm
[22]	2019	Availability	Use high availability architecture based on OpenStack
[23]	2018	Availability	The current snapshot scheme and HDFS

3. Attacks and protection in cloud of things CoTs

3.1 Threats and attacks in CoTs

The research [24] designs a framework that helps with the shifting of the processes that work under malicious edge devices towards the VHD, which increases the security and adaptiveness within fog layers. It utilizes three existing

concepts to work effectively, and they include the Markov model, Intrusion Detecting Systems (IDSs) as well as Virtual Honeypot Devices (VHDs) for the identifications of malicious edge devices within the atmosphere of fog computation. The system's ability to protect is put to the test by attempting to breach the virtual atmosphere made with the use of Openstack as well as Microsoft Azure. It was found that the threats were successfully identified, and false IDS alarms were significantly reduced.

This paper [25] aimed at classifying traffic as either normal or abnormal flows using Support Vector Machines (SVMs) for the prediction of past activities that may not be considered normal. Network traffic was classified against DDOS attacks among predefined parameters. SVMs and Ks were applied for the classification of each packet in a highly accurate manner. Extensions of this investigation can be carried out through the application of AI and other algorithms that can help prevent unwanted traffic at the ports.

This investigation [26] attempts to tackle DDoS attacks that mischievous IoTs trigger. The cloud and software-defined network (SDN) are utilized for mitigation of DDoS attacks on IoTs servers. The concept they introduced is called LEarning driven Detections and Improvements (LEDEMs) and it helps with detecting and mitigating DDoS attacks with the use of partially administered artificially intelligent algorithms. It can accurately detect up to 96.28 percent of all DDoS attacks and can put a stop to DDOS attacks even if the servers face an attack from wireless IoTs.

The paper [27] includes a discussion regarding breaches and protection against the same on Cloud Assisted ITs.

Jamming attacks are targeted towards a wireless network and would require communications to be hindered through the transmittance of undesirable communications that contaminate the original messages or the blocking of the messages from arriving at their target locations. Detection and prevention of such breaches can be done using numerous techniques that are related to cryptographic as well as stenographic algorithm usage. Prevention techniques can range from the development of a reputation or credit system to communicative intense acknowledgment models.

Sybil attacks are when nodes maliciously appear with more than one identity within a network. Here, the attackers aim to use their breaches to affect whatever they desire. Prevention methods include the employment of methods that help validate the identities of each node within the network. Additionally, certificates, attenuations of privileges, tests for resources, verifying locations, and authenticating messages are required to recognize the identity of a node before allowing it to run on a network.

Data tempered attacks are when the attackers attempt to obtain the private information of other users. The investigation [28] involves constructing a message forwarding framework that preserves the user's privacy for opportunistic CoTs so that the protection of personal information can be guaranteed, and transmissions can be improved professionally. The cloud server was architecture to accommodate a dual-layer model that helped in improving efficient communications between clients. The integration of secure mobility predicting algorithms with route deciding processes allow for the effective protection of personal information. The investigation also discusses the integration of attribute-based algorithmic cryptography that allows communication that resists breaches. Implementation of this system helps to make packet transmissions more efficient and also helps to guarantee a secure and effective network during potential breaches.

The paper [29] suggests applying IoT-NETZ security, operating on a software-sized networking paradigm for the detection and effective mitigation of breaches that depend on spoofs. The investigation then discusses a potential strategy, which involves the protection of IoTs from breaches in cloud infrastructure with the use of practical mechanics. Result found this method to be effective in eliminating the network overheads for per-flow processing tasks when applying controllers, validating sources, and reverse tracking all traffic of the generated network traffic.

3.2 Protection in CoTs

The paper [30] single-point defensive capabilities and cooperative defensive mechanisms are formulated by constructing active defensive systems to ensure that the IoT services are secure for various attack scenarios of cloud, which can help with the improvement of the defenses in the event of breaches of greater complexity or illegal actions that require the changing of passive defenses to active defenses. Additionally, fixing the weaker connections within the systems that monitor security and provide early warnings. The proposed solutions can be integrated for the significant improvement of what IoTs are capable of secure networks, mobile interconnections, secure data, confrontations, and perceptions.

The article [31] includes a proposal for defenses for cloud-based IIoT. A DNN is synthesized for the accurate resistance against breaches and guaranteeing confidentiality depending on the utilized modified federated learning frameworks. The article concludes by demonstrating how their approaches show an improvement within the overall defenses when faced with numerous breaches as well as the accurate detection of misbehaving DNNs as a result of newer breaches.

The researchers [32] introduce a proposal that discusses the potential of network-based intrusion detecting systems (NIDSs). For SDNs within IoTs, SeArch is usually used. An investigation must then be conducted with regard to the processing logic of the systems that include how they initialize, operate runtimes, and update databases. Solutions are then implemented in a detailed manner within SDN atmospheres where several different aspects are studied.

The final step would be to evaluate and conclude with what the methods yielded, and it was found to perform outstandingly when detecting and mitigating anomalies and dealing with bottleneck problems within in the SDN-based cloud IoT networks.

Table 2: Attacks and protection in Recent Papers Related to CoTs Security

Ref	***Year***	Threats &Attacks	Approach &Prevent
[24]	2018	malicious edge device	Use the Markov Model, Intrusion Detection System (IDS), and Virtual Honeypot Device (VHD)
[25]	2018	DDOS attack	-Use Support Vector Machine Algorithm(SVM)
[26]	2020		(LEDEM) using machine-learning algorithm.
[27]	2018	Jamming Attack	Use the cryptography and steganography algorithms.
		Sybil Attack	Use identity-based node verification, trusted authentication, resource proof, authority mitigation, location verification, authentication, and message delivery.
[28]	2018	Data tempered attack	Use attribute-based cryptographic algorithm.
[29]	2020	spoofing-oriented network attacks	Use mechanism to protect wide-scale IoT networks.
[30]	2020	different attack scenarios of "cloud, management	Use cooperative defense mechanism.
[31]	2020	adversarial attacks	Use a novel federated defense approach.
[32]	2019	bottleneck problem	Use intrusion detection system (NIDS) architecture.

4 Discussion

Numerous methods have been mentioned for the protection of user privacy from different papers and other literature. These must now be discussed and compared, which is what will be done in this section.

Confidential data can be guaranteed in CoTs using cloaking algorithms that broaden the user's location make it more difficult for an attacker to obtain information. This is paired with the Mobility Markov chain concept and both help with the avoidance of leaked private information. Here, a common driver was utilized to extend CoTs functions and implementation took place using OpenStack to manage and Orchestrate (MANO) the same. It was very successful in ensuring confidentiality by authenticating using FPGAs, which offers ways in which symmetric session keys can be established throughout FPGAs. More literature referred to BCSABEs that involve the replacement of conventionally centralized servers with decentralized blockchain systems as the controller and generator of threshold parameters, withdrawal of users, and manager of keys. It is an improved alternative to encrypting with algorithmic ABEs as the mathematics are highly complex and one must make numerous estimations which is intolerable when controlling IoTs.

Users were authenticated using numerous methods, including CLPAEKSs which is more secure and efficient. Here, KGCs generate each parameter as well as a section of a user's personal encryption key depending on their credentials. Specific data is then extracted from the files with this encrypted key where CLPAEKSs cipher text is formed. Additional algorithms are then utilized to transfer the files to cloud servers attached to the ciphertext. Receivers can then utilize their confidential key along with the public one of the sender for the generation of trapdoor Tws for every keyword which is then sent back to the servers. The server then begins searching and returning the files that have the mentioned data. Other articles use trust frameworks to test the IP/MAC addresses of devices that have an active connection to IoTs. They then utilize specific methods of testing these credentials and grant access depending on the user.

These methods can include facial or vocal recognition, passcodes, and even unique pattern recognition. Other papers propose authentication using multi-factor methods and lightweight cryptographic methods that involve sorting any device based on the sensitivity of the information stored within them. Devices with higher sensitivity face encryption with RC6 and the feistily encrypting algorithm. Such information is then transferred to confidential cloud servers to ensure that the data is secure. Devices with lower sensitivity face encryption with AESs where they get transferred into publically available servers. Any individual that attempts to access this data would have to undergo 3 steps to authenticate their access, and they are usernames, passwords, and biometric data. It was found that this proposal's performance was superior to FCSs, CPABEs, and MCPABEs.

Sometimes, more than one mechanism is required to prevent unwanted access. One researcher focused on using SEMACSITs in 8 parts. The cloud servers would first provide facilities to store data as well as allow users to facilitate the management of required files. DOs are then used for the encryption of this shared data to ensure that only specific users have the ability to access the same. This is done using ciphertext and keys uploaded to the servers.

Finally, the encrypted files are decrypted using DUs after verifying that the credentials match the list of permitted users. Other papers recommend the usage of a symmetric and asymmetric signature within a JSON token.

Integrity is achieved using numerous methods in the literature. An example is where short signature algorithms are utilized to validate the integrity of data. This is done by pairing bi-linearly, which means that BLSs are more overhead in comparison. MHTs are also known to be used depending on the hash functions. This involves the construction of SGMHTs that integrate MHTs and scapegoat trees. Ranking related data would be integrated o the nodes for the MHTs, after which maintenance of balances can be done with the use of rotation-less, self-balance concepts. Hierarchical logs are utilized for efficient functioning and the lack of extra overheads is the main distinguishing feature of the system.

Ensuring that all data is available at all times is a very important aspect within CoTs. Faults are detected and recovered based on the configurations made by template-based server models which depend on the characteristic features mentioned to make resources available. Other papers made modifications to HDFSs so that the replica quantities made when during each snapshot would increase so that more would be available to a user at any given period. This would also mean that improvements can be made to files of greater priority in each snapshot.

Several papers have also mentioned mechanisms for protection against attackers. This investigation covers a few examples and reviews countermeasures taken to prevent malicious breaches. Some researchers used the Hidden Markov Model to get accurate calculations of how likely it was for malicious edge devices to be present within the fog computational environment using data from previous attacks. Essentially, the model deliberates the expected actions from an edge device where the attack is initially tagged based on its nature and the shifting probabilities (SPs) are determined. The processed data is then used to determine the need for a VHD shift based on plotted graphs. The transition graphs would differ for all devices and updates are constantly made using Viterbi algorithms. The hidden states are then discovered using the algorithms by analyzing the activity sequences taken on the users' end. Once identification is successfully conducted, the attack is parried. The framework also reduces false IDS alarms.

Some papers suggest the prevention of DDOS attacks by classifying traffic allowed within their networks. This classification can occur with the help of Supporting Vector Machine algorithms that assist with the detection, classification, and analysis of malicious content from IoTs that use XOICs as a method of directing DDOS attacks from numerous sources to a single location. The content analyzed can include the sources, destinations, and packet counts of all the attacks. Wireshark is an efficient application to collect this data. The data is then analyzed and classified depending on the type of the IoT attack using same algorithms.

The next aspects that are considered in a lot of the literature are attacks on the securities of the CoT resources. Jamming attacks involve the targeting of a wireless network and would require communications to be hindered through the transmittance of undesirable communications that contaminate the original messages or the blocking of the messages from arriving at their target locations. This can be countered with a reputation system, credit system, and communicative intense acknowledgement that stop such attacks from taking place. Sybil attacks are when nodes maliciously appear with more than one identity within a network. This can be prevented with the use of certificates, attenuations of privileges, tests for resources, verifying locations, and authenticating messages.

Other solutions mentioned in the literature used for this investigation were for the protection of CoTs from attacks on their cloud-based architecture. The solutions involved using NETZ, which would be operating on software-sized networking paradigms for the detection and effective mitigation of breaches that depend on spoofs. Such methods enable the protection of IoTs with the use of Software-defined Wireless Networks. The concept helped with eliminating the network overheads for per-flow processing tasks when applying controllers, validating sources, and reverse tracking all traffic within the CoT networks.

One paper mentioned the effectiveness of defensive methods known as FDA3 which aggregates defense-related data from numerous locations with the help of deep learning methods. Attack modules are utilized for the recording of data on the most recent breaches within IoTs, depending on their location and type. It is responsible for managing a large database of every detected breach. Collection of this data occurs from an external producer unrelated to the institution. If a breach is detected by the modules, the devices must begin downloading the necessary schemes to restrain the attackers. This is known to make a substantial improvement in the method used to defend against such breaches.

Data tempered attacks are also quite prevalent and approaches that attempt to put a stop to such breaches are necessary. One paper suggests the usage of symmetric algorithms when encrypting any message between devices, where the keys for the messages are encrypted using local algorithms. The attribute-based algorithms utilize public keys for their encryptions as well as access trees depending on the predefined credentials of a user. Decryption is then done by the receivers who use their confidential keys to understand the message. These keys remain confidential as they are generated only based on the same predefined credentials mentioned for the receiver. This means that the interception of these messages cannot take place at a node either since the credentials would not match that which was

already defined and the messages would not have been possible to decrypt.

The final method of prevention was using network-based intrusion detecting systems (NIDSs) that possess intelligence and the ability to collaborate. For SDNs within IoTs, SeArch is usually used. An investigation must then be conducted about the processing logic of the systems that include how they initialize, operate runtimes, and update databases. Solutions are then implemented in a detailed manner within SDN atmospheres where several different aspects are studied. Evaluating the results produced showed this method to perform outstandingly when detecting and mitigating anomalies and dealing with bottleneck problems within SDNs of CoTs.

5 Conclusion

There is no question about the fact that IoTs and CC, when integrated, form something very beneficial with numerous helpful ways in which they can be applied, as an IoTs is responsible for the generation of large stores of data which the cloud computing processed, stored and presented in the future. Remaining secure is an essential part of such concepts as it is one of the aspects that receive the highest priority. The lack of storage within an IoT would hinder the generation process, which would lead to issues related to remaining secure and confidential. Currently, there are numerous benefits present stemming from the integration of both IoTs and CC that prevent such issues from ever taking place. Thus, the main significances are implementing measures that ensure the entire operation remains secure with reliability along with some additional attributes such as remaining confidential, available, and accessible. This paper covered numerous different searched recent research submitted through other researchers about how to achieve security requirements and the mechanisms used for that. Therefore, the contents of this paper can be used as assistance for readers, if they wish to understand the dangers of CoTs as well as how they can use it professionally. Additionally, we introduced several different attacks that targeting a CoTs environment and how to protect from them from these attacks.

Acknowledgments

References

[1] Atlam, H. F., Alenezi, A., Alharthi, A., Walters, R. J., & Wills, G. B. (2017, June). Integration of cloud computing with internet of things: challenges and open issues. In 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) (pp. 670-675). IEEE.

[2] Paul, A., & Jeyaraj, R. (2019). Internet of Things: A primer. Human Behavior and Emerging Technologies, 1(1), 37-47.

[3] Farahzadi, A., Shams, P., Rezazadeh, J., & Farahbakhsh, R. (2018). Middleware technologies for cloud of things: a survey. Digital Communications and Networks, 4(3), 176-188

[4] Tadapaneni, N. R. (2018). Cloud Computing: Opportunities and Challenges. *Available at SSRN 3563342*.

[5] Bhawiyuga, A., Kartikasari, D. P., Amron, K., Pratama, O. B., & Habibi, M. W. (2019). Architectural design of IoT-cloud computing integration platform. *Telkomnika*, *17*(3), 1399-1408.

[6] Pacheco, L., Alchieri, E., & Solis, P. (2017, April). Architecture for Privacy in Cloud of Things. In ICEIS (2) (pp. 487-494)

[7] Alabdulatif, A., Khalil, I., & Ahmed, S. H. (2018). Integration of Internet of Things (IoT) and Cloud Computing: Privacy Concerns and Possible Solutions. *Integration*, *2017*.

[8] Li, W., Santos, I., Delicato, F. C., Pires, P. F., Pirmez, L., Wei, W., & Khan, S. (2017). System modelling and performance evaluation of a three-tier Cloud of Things. Future Generation Computer Systems, 70, 104-125.

[9] Riyaz Belgaum, M., Soomro, S., Alansari, Z., Alam, M., Musa, S., & Suud, M. M. (2018). Challenges: Bridge between Cloud and IoT. *arXiv e-prints*, arXiv-1803.

[10] Sahmim, S., & Gharsellaoui, H. (2017). Privacy and security in internet-based computing: cloud computing, internet of things, cloud of things: a review. Procedia computer science, 112, 1516-1522.

[11] Choudhury, T., Gupta, A., Pradhan, S., Kumar, P., & Rathore, Y. S. (2017, October). Privacy and security of cloud-based internet of things (IoT). In 2017 3rd International Conference on Computational Intelligence and Networks (CINE) (pp. 40-45). IEEE.

[12] Tian, Y, Kaleemullah, M. M., Rodhaan, M. A., Song, B., Al-Dhelaan, A., & Ma, T. (2019). A privacy preserving location service for cloud-of-things system. Journal of Parallel and Distributed Computing, 123, 215-222.

[13] Al-Asli, M., Elrabaa, M. E., & Abu-Amara, M. (2018). FPGA-based symmetric re-encryption scheme to secure data processing for cloud-integrated internet of things. *IEEE Internet of Things Journal*, *6*(1), 446-457.

[14] Liu, S., Yu, J., Xiao, Y., Wan, Z., Wang, S., & Yan, B. (2020). BC-SABE: Blockchain-Aided Searchable Attribute-Based Encryption for Cloud-IoT. *IEEE Internet of Things Journal*, *7*(9), 7851-7867.

[15] Wu, B., Wang, C., & Yao, H. (2020). Security analysis and secure channel-free certificateless searchable public key authenticated encryption for a cloud-based Internet of things. PloS one, 15(4), e0230722.

[16] Abualese, H., Al-Rousan, T., & Al-Shargabi, B. (2019). A New Trust Framework for E-Government in Cloud of Things. International Journal of Electronics and Telecommunications, 65.

[17] Atiewi, S., Al-Rahayfeh, A., Almiani, M., Yussof, S., Alfandi, O., Abugabah, A., & Jararweh, Y. (2020). Scalable and secure big data IoT system based on

multifactor authentication and lightweight cryptography. *IEEE Access*, *8*, 113498-113511.

[18] Xiong, S., Ni, Q., Wang, L., & Wang, Q. (2020). SEM-ACSIT: secure and efficient multiauthority access control for IoT cloud storage. IEEE Internet of Things Journal, 7(4), 2914-2927

[19] da Silva Martins, W., Estrella, J. C., Bruschi, S. M., de Azevedo, L. J. D. M., & Andreazi, G. T. (2020, October). Performance evaluation for signing JSON tokens in access control for the cloud of things. In 2020 IEEE Cloud Summit (pp. 72-78). IEEE.

[20] He, J., Zhang, Z., Li, M., Zhu, L., & Hu, J. (2018). Provable data integrity of cloud storage service with enhanced security in the internet of things. *IEEE Access*, *7*, 6226-6239.

[21] Zhu, H., Yuan, Y., Chen, Y., Zha, Y., Xi, W., Jia, B., & Xin, Y. (2019). A secure and efficient data integrity verification scheme for cloud-IoT based on short signature. IEEE Access, 7, 90036-90044.

[22] Yang, H., & Kim, Y. (2019). Design and implementation of high-availability architecture for IoT-cloud services. Sensors, 19(15), 3276.

[23] Yeh, T., & Tu, Y. (2018, December). Enhancing data availability through automatic replication in the hadoop cloud system. In 2018 9th International Symposium on Parallel Architectures, Algorithms and Programming (PAAP) (pp. 86-93). IEEE.

[24] Sohal, A. S., Sandhu, R., Sood, S. K., & Chang, V. (2018). A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments. Computers & Security, 74, 340-354.

[25] Gurulakshmi, K., & Nesarani, A. (2018, May). Analysis of IoT Bots against DDOS attack using Machine learning algorithm. In *2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI)* (pp. 1052-1057). IEEE.

[26] Ravi, N., & Shalinie, S. M. (2020). Learning-driven detection and mitigation of DDoS attack in IoT via SDN-cloud architecture. IEEE Internet of Things Journal, 7(4), 3559-3570

[27] Alsaidi, A., & Kausar, F. (2018, September). Security attacks and countermeasures on cloud assisted IoT applications. In 2018 IEEE International Conference on Smart Cloud (SmartCloud) (pp. 213-217). IEEE.

[28] Wang, X., Ning, Z., Zhou, M., Hu, X., Wang, L., Hu, B. ... & Guo, Y. (2018). A privacy-preserving message forwarding framework for opportunistic cloud of things. IEEE Internet of Things Journal, 5(6), 5281-5295.

[29] Mohammadnia, H., & Slimane, S. B. (2020, April). IoT-NETZ: Practical Spoofing Attack Mitigation Approach in SDWN Network. In 2020 Seventh International Conference on Software Defined Systems (SDS) (pp. 5-13). IEEE

[30] Li, F., Zhang, K., Chen, S., Yang, H., & Wang, B. (2020, November). Research on Key Technologies of Active Defense for Distribution Internet of Things Service Security. In 2020 IEEE International Conference on Information Technology, Big Data and Artificial Intelligence (ICIBA) (Vol. 1, pp. 676-679). IEEE.

[31] Song, Y., Liu, T., Wei, T., Wang, X., Tao, Z., & Chen, M. (2020). Fda3: Federated defense against adversarial attacks for cloud-based iiot applications. IEEE Transactions on Industrial Informatics.

[32] Nguyen, T. G., Phan, T. V., Nguyen, B. T., So-In, C., Baig, Z. A., & Sanguanpong, S. (2019). Search: A collaborative and intelligent nids architecture for sdn-based cloud iot networks. IEEE access, 7, 107678-107694