Protection Mechanism against Software Supply Chain Attacks through Blockchain

Muhammad Zeeshan Malik (MSIS-20)
Information Security Department
Military College of Signals
Rawalpindi, Pakistan
muhammadzeeshanmalik88@gmail.com

Syed Zain Ali Bukhari (MSIS-20)
Information Security Department
Military College of Signals
Rawalpindi, Pakistan
syedzainali07@gmail.com

2023 International Conference on Communication Technologies (ComTech) | 979-8-3503-3721-1/23/$31.00 ©2023 IEEE | DOI: 10.1109/ComTech57708.2023.10164932

***Abstract*— Software supply chain attack is exceptionally fatal, overwhelmingly rapid, and almost effortless on the part of the attacker. A single compromise or hack can lead to multiple businesses sufferings because suppliers and providers have a vast user network. Protection against software supply chain attacks is being achieved through some outdated concepts like honeytokens and privileged pathway, but an integrated and proper mechanism is still lacking. In recent years, blockchain technology represents a fundamental shift that can replace conventional business models that rely on third parties for trust. This paper proposes a protection mechanism through validity concept with the implementation of blockchain to retain an immutable and trustworthy record of propagating payload (i.e., official update) that is transmitted across the supply chain systems. Blockchain can be used to circumvent these supply chain attacks by keeping a digital log of all propagating information. Each block contains the information regarding validity of propagating data, based on this an official update can be accepted or rejected.**

Keywords—SolarWinds, Honeytoken, Privileged Path

I. INTRODUCTION

Software supply chain attacks are a new type of threat that primarily targets software developers and providers. The purpose is to get access to source code, development processes, or update mechanisms to disseminate malware via infecting legitimate applications "Fig. 1". [1], [2]

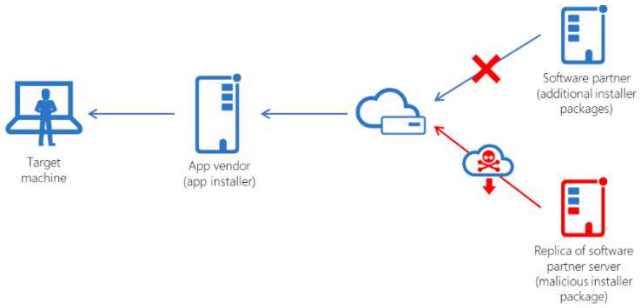

Fig. 1. Software supply chain attack

Software supply chain attacks can have multiple sources one of the sources is open-source software supply chains where anyone may contribute to the development process. Commercial software products are another source because organizations utilize the same software providers and suppliers. An attacker can get access to many targets if they can enter a software company's system or defect the integrity of their product. Foreign-sourced threats are also the source where the government has extensive control over what private enterprises produce. Software items may contain malware that the government instructed to include. [3]

According to the analysis, 33% of 24 established software supply chain attacks were recorded in 2020 and 66% from January 2021 to early July 2021. The trend predicts that supply chain attacks will be four times more common in coming years. It is being preferred in cybercriminal community due to following reasons:

- Extremally difficult to detect as it uses all legitimate resources and processes.
- Exceptionally fatal and remarkably rapid (like Domino Effect "Fig. 2", almost unstoppable during propagation through conventional methods).

Fig. 2. Domino Effect

- Comparatively easier to craft and execute than other attack strategies.

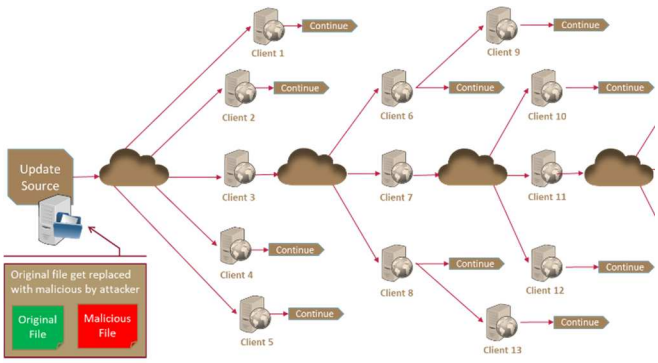

Fig. 3. Basic Attack Procedure

As shown in "Fig. 3' only the Malicious File (even this file is with official certificate) is the effort made by attacker rest of the resources and processes which are being utilized in this attack are legitimate and genuine. By 2025, 45% of organizations around the world will have experienced this attack.

II. LITERATURE REVIEW

Based on some well-known and recent examples of software supply chain attacks, trends and statistics are being extracted. Keeping the above in view, problems and

979-8-3503-3721-1/23/$31.00 ©2023 IEEE

weaknesses have been identified which are leading towards escalation in these attacks. A unified and proper solution / protection mechanism is being proposed to mitigate software supply chain attacks by incorporating existing solutions as a validation algorithm with blockchain in this section.

A. Recent Incidents

Five of the most recent and known supply chain attacks are being scrutinized. These instances are chosen because of the tremendous influence they have on the community, and they have emphasized specific qualities that are relevant and significant for analytical purposes, which would lead to problem identification.

- *SolarWinds attack:* This attack was one of the most complex, well-crafted, and devastating supply chain cyber-attacks in history. The organization's dynamic library file was compromised because of this attack "Fig. 4". Unfortunately, the virus was disseminated to all customer networks by an unknowing vendor. Threat actors employed DGAs (Domain Generation Algorithm) to resolve sub-domains of the C2 domain avsvmcloud.com while staying low to avoid raising suspicions on outbound traffic. [4]

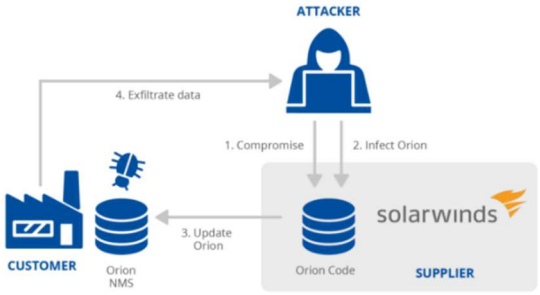

Fig. 4. SolarWinds Attack

The attacker stayed undiscovered by employing a variety of techniques, including a temporary file replacement approach in which they replaced a genuine utility "Fig. 5" with their own, executed their payload.

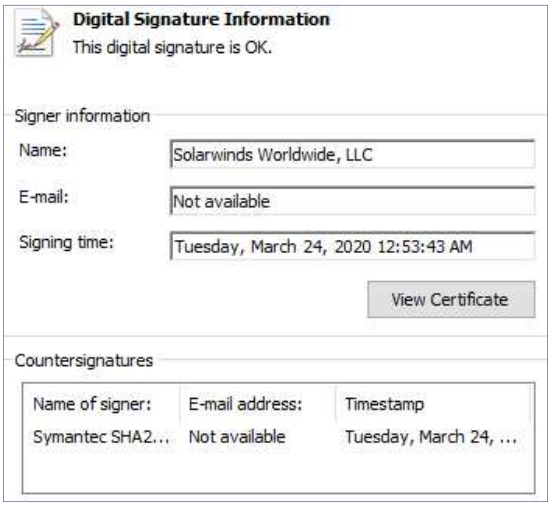

Fig. 5. Official update which was signed on 24 March 2020

- By only utilizing IP addresses from the same country as the victim.
- Continue to check for the presence of security controls or scanning tools and then disable them by modifying registry keys.
- By employing several credentials for lateral movement and remote access.[5]

Malware's course of action was as follows:

Fig. 6. SolarWinds Attack Course of Action

An in-depth analysis revealed that attackers acquired access "Fig. 6" to the SolarWinds network via zero-day vulnerability in a third-party application. [6]

- *Mimecast, cloud cybersecurity services:* Mimecast is a provider of cloud-based cybersecurity services. It offers email security services through their Microsoft 365 accounts, which connects their clients' protection to the Mimecast servers. It was discovered in January 2021 that attackers had infected Mimecast (through the SolarWinds supplier) "Fig. 7".

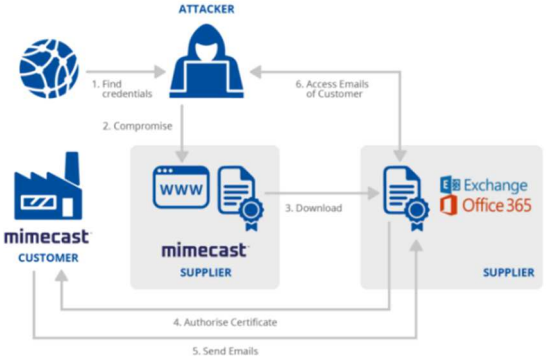

Fig. 7. Mimecast, Cloud Cybersecurity Services

Attackers obtained a Mimecast official certificate used by end-users to access Microsoft 365 services, allowing them to intercept network connections and login to Microsoft 365 accounts to steal information. The APT29 gang was blamed for the attack. The supplier's breach has purportedly been tied to SolarWinds, although there is no specific evidence to back this up.[6]

- *Kaseya, ransomware-infected IT management services:* Kaseya is a software service provider that specializes in remote monitoring and management technologies. It provides its clients with VSA (Virtual System / Server Administrator) software that they may download and use on its own cloud servers. [6]

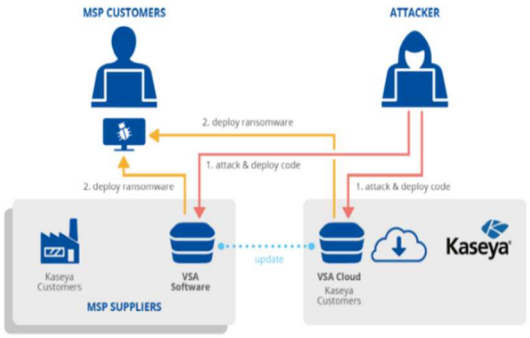

Fig. 8. Kaseya, Infected IT Management Services

MSPs (Managed Service Providers) can employ the VSA software on-premises or license Kaseya's VSA cloud servers. MSPs, in turn, provide a variety of IT services to other clients. Attackers exploited a zero-day vulnerability in Kaseya's own systems (CVE-2021-3011632) in July 2021, allowing the malicious actor to remotely execute instructions on Kaseya's customers' VSA equipment "Fig. 8". Kaseya can remotely update all VSA servers, and on Friday, July 2, 2021, an update was dispersed to Kaseya clients' VSAs that executed code from the attackers.[6]

- *Ledger / hardware wallet:* Ledger is a firm that supplies cryptocurrency hardware wallet technology. Attackers obtained legitimate credentials to access Ledger's e-commerce database in July 2020 "Fig. 9".

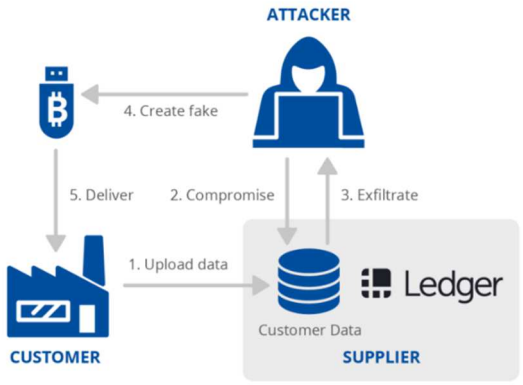

Fig. 9. Ledger / Hardware Wallet

The stolen information was made public on an online forum. Attackers used the stolen data for online phishing and extortion of users[6]

- *SITA Passenger Service System:* SITA is an aviation information technology and transportation information corporation. In March 2021, it was discovered that attackers had infiltrated SITA systems to get access to passenger information from SITA customers. Some SITA clients, including Air India, Singapore Airlines, and Malaysia Airlines, have also disclosed data breaches "Fig. 10". On these rumors of leaking data on the Internet, Air India declared that its networks had been compromised and data had been taken. The penetration of Air India's internal networks was apparently linked to the SITA incident. It is still uncertain how the attackers got access to the SITA systems. [6]

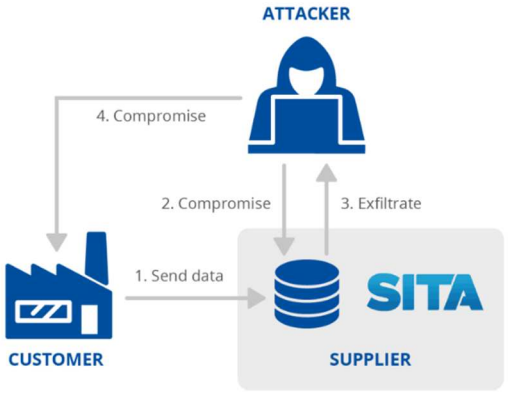

Fig. 10. SITA Passenger Service System

B. *Existing Prevention Methods*

This section is discussing already in placed methods to prevent software supply chain attacks:[7], [8]

TABLE I. EXISTING PREVENTION METHODS

Method	Description	Advantages
Implementation of Honeytokens to find out "Privileged Pathway" [9]	• Placement of fake resources acts as important data to alert the owners about attack without compromising • To identify the attack sequence as attacker will try to access the sensitive data through privileged accounts [10]	• Identify the attack strategy • Advance alert • Increase attack dictionary • There are great chances that location and identity of the hacker can be exposed
Implement a Zero Trust Architecture	Consider each in and out bound activity is evil, apply control through strict policies	• Stop letteral movement • Proactive model
Maintaining history / records of data leaks		Track the trust and validity level of a particular source

C. *Problems and Shortcomings in Existing Methods*

- *Insufficient security frameworks:* Researchers discovered that prior frameworks used to guard against software supply chain threats are no longer adequate. In other words, firms must devise innovative ways to protect themselves against supply chain dangers.
- *Reliance on 3rd party for protection:* All protection mechanisms which are in place are purely centralized in nature. These central mechanisms have their own policies and rules which are mostly in favor of their own stacks. As they are completely out of control with respect to end user, everything is dependent upon centralized authorities so

manipulation and exposure of user data may happen. These supply chain attacks are totally exploitation of end user trust. So there must be a decentralized mechanism which can protect end user data.

- *Inadequate identification and encryption of sensitive data:* It has been noted as a serious issue that corporate companies are not identifying and prioritizing their essential assets. It is highly suggested by standards that sensitive data be encrypted and secure. Businesses can limit the scope of any supply chain attacks that do occur. Even if bad actors get access, they will be unable to exploit secured assets.
- *Software vulnerabilities:* Strict cybersecurity criteria are not met at all stages of the software supply chain system when the software is in development. Any penetration, security breach, or open-source network can result in a supply chain attack.
- *Inadequate security analysis:* Today's software supply chain software world is more complicated than ever. Companies, on the other hand, do not perform in-depth analyses of supplier security measures. They must deconstruct internal operational procedures to guarantee that all departments are on the same page when it comes to security. [6]

III. NOVEL SOLUTION

Protection against software supply chain attacks is being achieved through some outdated concepts i.e., honeytokens and privileged pathway, but an end-to-end and proper mechanism is still missing. In recent years, blockchain technology represents a fundamental shift that can disrupt or perhaps replace conventional business models that rely on third parties for trust. Unfortunately, software supply chain attacks rely on the legality of a seller, in whom everyone has faith, but attackers might misuse this confidence. When an attacker inserts harmful code into a legitimate update or software, its credibility and trust level become questionable, to check this update or program while it is propagating, a decentralized approach or process might be helpful in this context. To implement this there must be a decentralized mechanism to confirm its trustworthiness and validity in a more unified and proper manner.

A program called "Validation" “Fig. 11” will be executed on users' machines to automatically assess the legitimacy of updates or software using techniques such as the honeytokens and privileged pathway and data loss ratio or any specific algorithm implemented by end users (scalable and flexible in terms of validity function because validity value will be assigned in percentage regardless of algorithm). When a legitimate update or software is provided from the Official Update Server, the information of its validity and trustworthiness will be propagated to user by user “Fig. 10”. All past transfer information will be contained in this ledger and this information will be kept on all users' PCs and cannot be changed because it is part of the blockchain process (immutability feature).

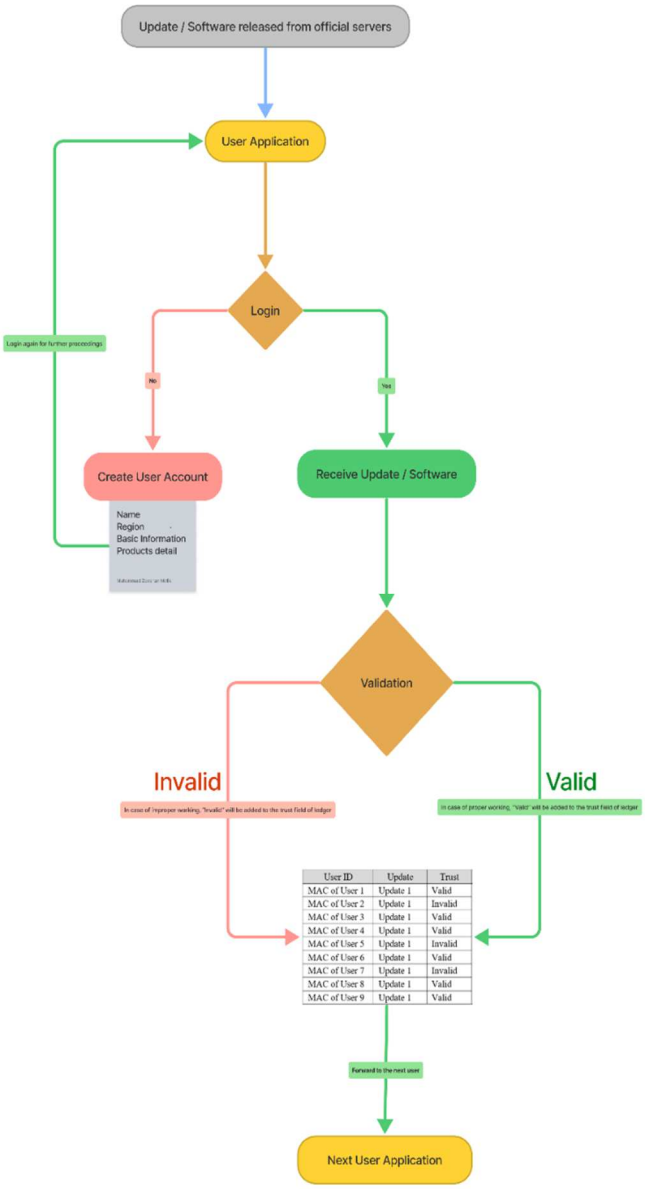

Fig. 11. Validation - Decentralized Approach

Validating Program / Algorithm
Broadly based on combination of following Checks:

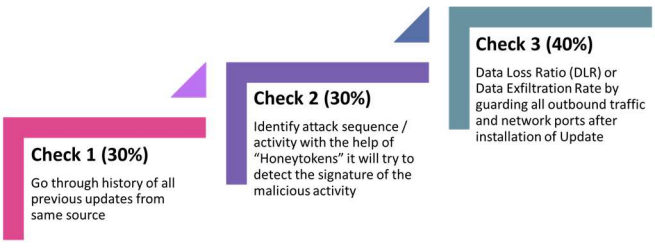

Fig. 12. Validation Algorithm

If the Validating Program / Algorithm “Fig. 12” detects a significant change, it will be considered as a malicious update, and the trust level will be shown as "Invalid”, and its validity level will be considered below 50% unless otherwise specified.

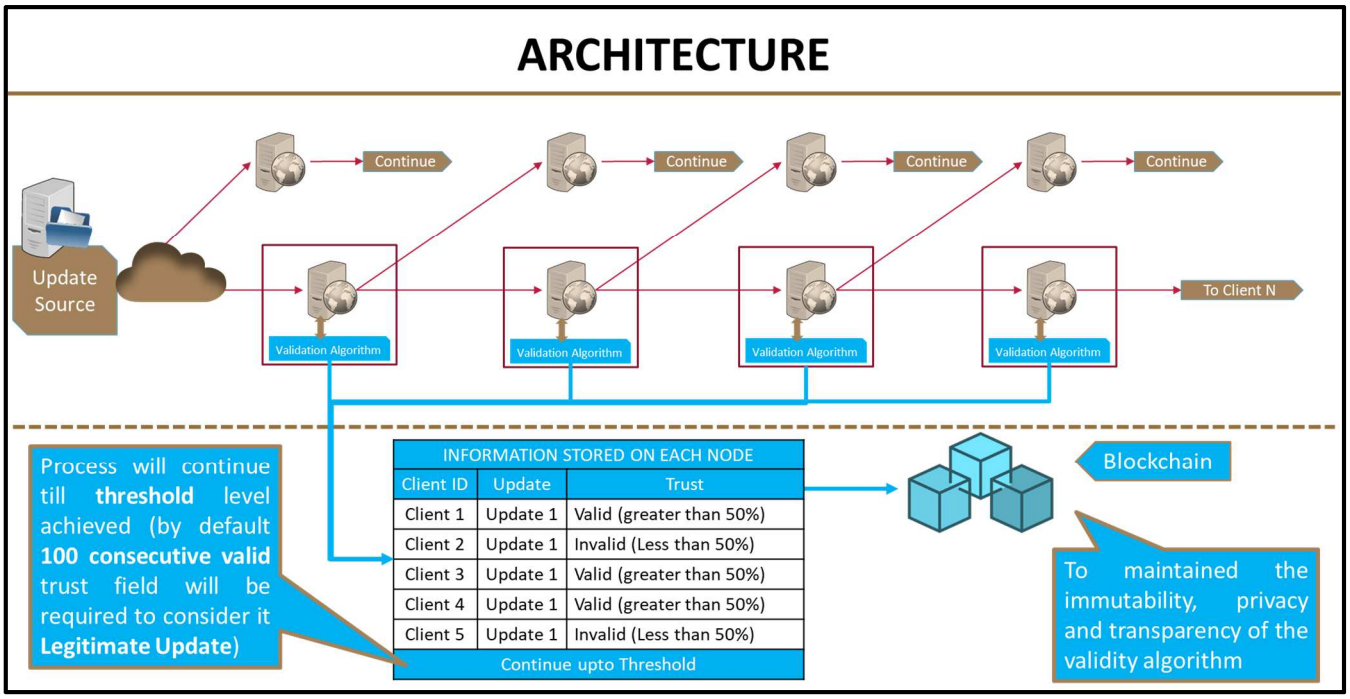

Fig. 13. Overall Architecture

A threshold will be set to make it valid, such as if 100 people consistently say it is a genuine update, it will be regarded valid, (complete architecture is at "Fig. 13"). Otherwise, it will be declared as an invalid, and the official server and the rest of the peers will be notified accordingly.

TABLE II. INFORMATION AVAILABLE ON EACH NODE

INFORMATION STORED ON EACH NODE			
Source	**Update**	**Timestamp**	**Trust = Valid / Total**
Source A	Update 1	Datetime 1	2 / 10 (Consecutive)
Source A	Update 1	Datetime 2	6 / 20 (Consecutive)
Source A	Update 1	Datetime 3	10 / 24 (Consecutive)
Source A	Update 1	Datetime 4	15 / 50 (Consecutive)
Source A	Update 1	Datetime 5	29 / 72 (Consecutive)
Continue upto Threshold = x / 100 **If x is greater than 50 (consecutive) then it will declare VALID** **If x is less than 50 (consecutive) then it will declare INVALID**			

IV. DISCUSSION

The combination of blockchain with software supply chain has come to the rescue of the trust paradigm, providing great opportunities, and resolving numerous issues. However, there are restrictions owing to integration's hurdles in the form of newly produced impediments, which offers doors for modern study ideas. Several important issues with blockchain are standing in the way of global and large-scale applications.

A. *Blockchain Standardization*

Blockchain is a new technology, it will take time to get standardization in the practical industry. Currently it is being implemented differently in various forms due to absence of standard. To achieve more reliability and long-term footprint in industry, it is highly necessary to have a common standard for Blockchain.[11], [12]

B. *Resources Constraints*

Blockchain is decentralized in nature, in this technology huge information and data must be maintained on multiple nodes at user end.[13] High processing power will also be required to retrieve stored information and data. This end user resource constraint is a major restriction in large-scale Blockchain applications. [14]

C. *Scalability Problem*

The existing internet infrastructure is huge in volume and there are around 5.03 billion internet users (statista, July 2022). It is a big hurdle to use blockchain as a global and large-scale application due to scalability issues.[15]

D. *51% Attack - Security Risk*

Although blockchain is decentralized in nature where a single entity cannot control everything. However, there is a possibility to gain more than 50% of the hashing power by a group who can control the Blockchain. An effective and fully executed 51% attack can lead to Denial-of-Service (DoS) and can restrict the nodes to access the Blockchain application. [16]

V. RECOMMNEDATION

The following design principles must be met to create a high-performance distributed and scalable supply chain network architecture with the goal of successfully integrating blockchain with supply chain systems to meet current and future challenges while also supporting new service requirements.

- *Efficiency and low latency:* The end system or node should function optimally.
- *Resilience:* In the event of a node failure, computing activities should be unaffected, and the system should continue to function using the remaining operational nodes.
- *Decentralized data storage:* The architecture should increase end-user storage capacity by utilizing blockchain storage capacity.
- *Scalability:* This is an important element to consider when creating a supply chain validity network that can handle future development in terms of the number of devices and the amount of data they create.
- *Simplicity of deployment:* All nodes should be able to join the network without requiring complex setups.
- *Data Integrity:* To maintain the quality and consistency of data in a decentralized environment, the integrated system must have a dependable built-in data verification mechanism.
- *Security:* One of the primary goals of implementing a new design architecture is to secure the network. As a result, data confidentiality and security must be effectively handled to enable a comprehensive design of the integrated system.
- *Data authenticity:* In a heterogeneous and decentralized environment, data exchanges need be verified and validated.
- *Privacy:* Blockchain should ensure the privacy of users' data. This ensures that network members' sent data is not being traced or manipulated.

VI. CONCLUSION

In this research it has been established that merging blockchain with software supply chain systems can provide superior detection mechanism and better reliability in terms of trustworthiness and legitimacy than without blockchain integration. Specially, this unified framework with the support of blockchain will provide opportunity to each node which is being involved in this process to play its role in verification of trustworthiness and legitimacy of official update or software. It is worth mentioning here that blockchain concept is going to revolutionize the internet, we just need to use it in a more useful way. However, several concerns and obstacles must be addressed, such as end-user node resource restrictions, scalability, security risk especially 51% attack.

VII. REFERENCES

[1] Alexander S. Gillis, "What is a Supply Chain Attack?," *TechTarget*, 2022. https://www.techtarget.com/searchsecurity-/definition/supply-chain-attack (accessed Nov. 05, 2022).

[2] Kevin Townsend, "Software Supply Chain Attacks Tripled in 2021," Jan. 20, 2022. https://www.securityweek.com/software-supply-chain-attacks-tripled-2021-study (accessed Nov. 05, 2022).

[3] Ben Kapon, "Three Types of Supply Chain Attacks Explained," *Cyberpion*, 2022. https://www.cyberpion.com/resource-center/blogs/types-of-supply-chain-attacks/ (accessed Nov. 05, 2022).

[4] Catalin Cimpanu, "FireEye, one of the world's largest security firms," Dec. 08, 2020. https://www.zdnet.com/article/fireeye-one-of-the-worlds-largest-security-firms-discloses-security-breach/ (accessed Nov. 05, 2022).

[5] Andrew Archer, Doug Bienstock, and Chris DiGiamo, "Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor," Dec. 13, 2020. https://www.mandiant.com/resources/blog/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor (accessed Nov. 05, 2022).

[6] Ifigeneia Lella, Marianthi Theocharidou, Eleni Tsekmezoglou, Apostolos Malatras, Sebastian Garcia, and Veronica Valeros, "Threat landscape for supply chain attacks July 2021 ENISA threat landscape for supply chain attacks about ENISA," 2021, doi: 10.2824/168593.

[7] Security Agency, "Defending Against Software Supply Chain Attacks," 2021. [Online]. Available: http://www.cisa.gov/tlp/.

[8] Edward Kost, "Ways to Prevent Supply Chain Attacks in 2022 (Highly Effective)," Aug. 11, 2022.

[9] Edward Kost, "Honeytokens as a Defence Against Supply Chain Attacks in 2022," Jun. 30, 2022.

[10] Edward Kost, "Privileged Access Management vs. Supply Chain Attacks in 2022," Jul. 11, 2022. https://www.upguard.com/blog/prevent-supply-chain-attacks-by-securing-pam (accessed Nov. 05, 2022).

[11] B. Carson, G. Romanelli, P. Walsh, and A. Zhumaev, "Blockchain beyond the hype: What is the strategic business value," 2018.

[12] Deshpande, Stewart, Lepetit, and Gunashekar, "Distributed ledger technologies/blockchain: Challenges, opportunities and the prospects for standards," May 2017.

[13] F. Knirsch, A. Unterweger, and D. Engel, "Implementing a blockchain from scratch: Why, how, and what we learned," Dec. 2019.

[14] Muhammad Khan and Salah, "IoT security: Review, blockchain solutions, and open challenges," vol. 82, May 2018.

[15] Zheng, Xie, Dai, Chen, and Wang, "Blockchain challenges and opportunities: A survey," vol. 14, 2018.

[16] Jake Frankenfield, "51% Attack: Definition, Who Is At Risk, Example, and Cost," Sep. 28, 2022.