Secure the 5G and Beyond Networks with Zero Trust and Access Control Systems for Cloud Native Architectures

Hisham A. Kholidy, Senior Member, IEEE, *Dept. of Networks and Computer Security, College of Engineering, SUNY Polytechnic Institute,* Utica, NY, USA. kholidh@sunypoly.edu

Keven Disen *Dept. of Networks and Comp. Security, SUNY Polytechnic Institute, Utica, NY*, USA. disenk@sunypoly.edu

Andrew Karam *The Air Force Research Laboratory (AFRL, RIGB),* Rome, NY, USA andrew.karam@us.af.mil

Elhadj Benkhelifa *Smart Systems, AI and Cybersecurity Research Centre, Staffordshire Univ., UK* e.benkhelifa@staffs.ac.uk

Mohammad A. Rahman *Dept of Electrical and Computer Engineering, Florida International University, USA* marahman@fiu.edu

Atta-ur Rahman *Dept. of Computer Science, , Imam Abdulrahman Bin Faisal University, Dammam, Saudi Arabia* aaurrahman@iau.edu.sa

Ibrahim Almazyad *Dept. of Electrical and Computer Engineering, Univ. of Arizona, Tucson, 85719*, AZ, USA almazyad@arizona.edu

Ahmed F. Sayed *Telecom Egypt, Transmission Dept., Fayoum, Egypt,* ahmed.darwesh.te@gmail.com

Rakia JAZIRI Paragraphe research Lab. Univ. of Paris VIII, France, rakia.jaziri@univ-paris8.fr

2023 20th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA) | 979-8-3503-1943-9/23/$31.00 ©2023 IEEE | DOI: 10.1109/AICCSA59173.2023.10479308

***Abstract*—5G networks are highly distributed, built on an open service-based architecture that requires multi-vendor hardware and software development environments, all of which create a high attack surface in the 5G networks than other proprietary fixed-function networks. Besides that, cloud-native architectures also present new security challenges. Cloud-native separates monolithic virtual machines into microservice pods, resulting in higher volumes of signaling and communication flowing through and between microservices. In addition, secure connections in monolithic applications have been replaced by untrusted communication between microservice pods, requiring additional cybersecurity capabilities. Access control systems were created to provide reliability and limit access to an organization's assets. However, due to technology's constant evolution and dynamicity, these conventional security systems lack the security to protect an organization's information because they were created to address access control for known users. For 5G based cloud native technology, these access controls need to be taken further by implementing a Zero Trust model to secure one's essential assets for all users within the system. Zero Trust is implemented in an access control system under the concept "Never Trust, Always Verify". In this paper, we implement zero trust as a factor within access control systems by combining the principles of access control systems and zero-trust security by factoring in the user's historical behavior and recommendations into the mix.**

Keywords—Access Control, Zero Trust Security, 5G, Cloud-native, RBAC.

I. INTRODUCTION

Technology has quickly turned from having physical servers to now being held in the cloud. This does not only speak to how technology has been evolving but to how quickly technology adapts to the environment. We can say that Covid-19 sparked the move from users working in a company building to WFH (Work From Home). Administrators adapted to this move by implementing and having users connect to VPNs, and/or migrating the company servers to the cloud to access them from anywhere. Yes, this can be useful for many companies, but it also poses a challenge. Users accessing the network or server in the cloud are no longer known users. Some unknown users are maintaining the data centers on which the company's server is being held. Applications and files are moved to network storage in the cloud. This indicates that a user working from home can be in an insecure network because it is no longer a secure enterprise network. However, Zero Trust Security can be implemented to give organizations the advantage of having a chance to secure their information. With this move, how we view Access Control also has to be changed. The conventional Access Control systems were suitable for the traditional type of system, not a 5G cloud native one. Therefore, we propose implementing Zero Trust into de-perimeterized networks in this paper by adding zero trust into access control models.

A. Zero Trust Security

Zero Trust Security is a security model to "help prevent unauthorized access to data and services coupled with making the access control enforcement as granular as possible" [1]. The challenge with moving a network to the cloud is that the perimeter-based network needs to meet the need for a remote and digitized environment. For this move to occur, this model is essential. In a traditional and physical system environment, "the authentication process establishes trust for the network access control (NAC) in authorizing a user/device to access data, assets, application, services (DAAS)," indicating that a user is authenticated and able to access confidential information with just their username and password. However, according to the Zero Trust Security principles, this process is not secure. Rather than establishing trust with a network based on someone's credentials, authentication is a prerequisite for access in a network that implements Zero Trust [1]. Zero Trust ensures that the subject is authentic and that the request for the resource that is needed is valid and within its constraints. This is done through the Policy Decision Point (PDP) and the Policy Enforcement Point (PEP), see Fig. 1. These policies take the subjects and constraints and ensure they are following the Separation of Duty [1].

Fig 1. Untrusted user/machine gaining access to an organization's assets [1].

The main phrase for this model is "Never Trust. Always Verify", hence the name zero trust. It does not trust a user or any endpoint system because, in a decentralized environment, that can bring a lot of vulnerabilities. Administrators have to know that they "cannot fully trust [a user's] local network connection [1]. In a remote setting, this seems to come up a lot, and most of the time, users do not have the resources to have a secure network. They also have to know that devices on the network may not be owned or configurable by the organization [1]. Users will buy any device not knowing some devices' security limitations. Zero Trust acknowledges these concerns and can create a secure remote perimeter-based network environment [1]. Rather than just trusting a user based on their credentials, it uses different models and tools for a user to authenticate and

979-8-3503-1943-9/23/$31.00 ©2023 IEEE
Authorized licensed use limited to: Indian Institute of Technology Hyderabad. Downloaded on May 27,2024 at 06:54:59 UTC from IEEE Xplore. Restrictions apply.

access information. It uses a Policy Decision Point (PDP) System, which contains a Policy engine, Policy Administrator, and Policy Enforcement Point (PEP), which communicate with each other to authenticate users into the network. The Policy Engine is the nucleus of this system because it evaluates the user's credentials and decides whether or not to grant the user access to the service or resource. Zero Trust Security also uses the Continuous Multi-factor authentication (CMFA) tool, which evaluates the authenticity of a user during an active session. This supports regular trust evaluation and allows an organization to see the user device and the network environment it is working in [2]. With organizations moving away from the traditional environment, they have to keep in mind the important strategy of deploying a Zero Trust system to a perimeter-based network. All of the organization's inventory has to be accounted for by the Policy Engine. This way, the system knows the users that must go through the trust evaluation and the resources and assets that must be protected. Then the system's policies, like risk management and business workflows, will have to be re-evaluated due to the fact that a perimeter-based network is different from a traditional network. This perimeter-based network will need stricter policies due to the fact that the architecture being implemented is "Zero Trust." The policy will contain the different circumstances or contexts (location of the device, trust level score, known user/device) that determine whether a subject will be granted or denied to a resource. This is retained within the Policy Engine because that is what manages the entire Zero Trust system. Once the policies, risks, and solutions are evaluated, it will be time to deploy the architecture and monitor any flaws that appear [1]. This migration and implementation will have to be done cautiously and for an extended period. As you see in the steps above, the Zero Trust Architecture is designed from the inside of the system's network to the outside.

B. *Access Control*

Within the organization's information security, administrators have to ensure that users are not only getting access to the company's internal network but are accessing the correct information. To do this, they implement Access Control Lists, which contain "a list of rules that specify who is granted or denied access to a particular object or resource" [3]. These lists can vary between Filesystem and Network lists. For Filesystem ACLs, users can be granted or denied to shared files/folders, network drives, and applications. Network ACLs filter the network by granting or denying packets based on their content or ports they are trying to reach. Access Control also allows administrators to keep a record of who has access to what and to satisfy an important security principle, Separation of Duty. According to the National Institute of Standards and Technology (NIST), Separation of Duty is where users should not have more privilege than what their duty entails. For example, an IT admin should not have access to create, edit, or delete paychecks. Since they have nothing to do with authorizing checks or the company's finance, they should not have access to do such things. Because of this security principle, Access Control has branched into many different models. The most common models implemented in organizations are Mandatory Access Control (MAC) and Role-Based Access Control (RBAC).

- **Mandatory Access Control** limits access to resources based on the sensitivity of the information that the resource contains and the authorization of the user to access information with that level of sensitivity [1].
- **Role-Based Access Control** model is based on the user's position within the organization. This model maps an employee to a role (job position). Within these roles, there are permissions that the specific role has, see Fig. 2. This satisfies the Separation of Duty, where all IT admins cannot have the same permissions to files/folders as payroll admins.

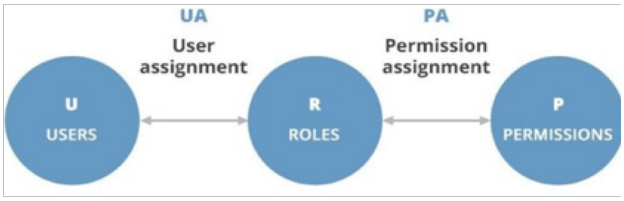

Fig 2. Role-Based Access Control model

The remainder of this paper is organized as follows. Section 2 presents the cloud native security. Section 3 describes the proposed ZTSF architecture and deployment model. Section 4 discusses the Zero Trust and Access Control Model. Section 4 introduces the main contribution of this paper. Section 5 discusses the experiments and simulation results. Finally, Section 6 draws some concluding remarks and outlines future work.

II. 5G Cloud Native Security Challenges

In this section, we briefly introduce the current security challenges and attacks against the 5G cloud native systems.

A. *Privilege escalation within a cloud-native service*

An attacker could exploit a public-facing service via an initial compromise, see Fig. 3, then use the service as a pivot for the next steps of the attack. In practical terms, an attacker could get inside a workload, find credentials in environment variables, and use those credentials to query the user management service for other credentials that could grant more privilege. When successful, the attacker can then change configurations, start new rogue services, and remove or

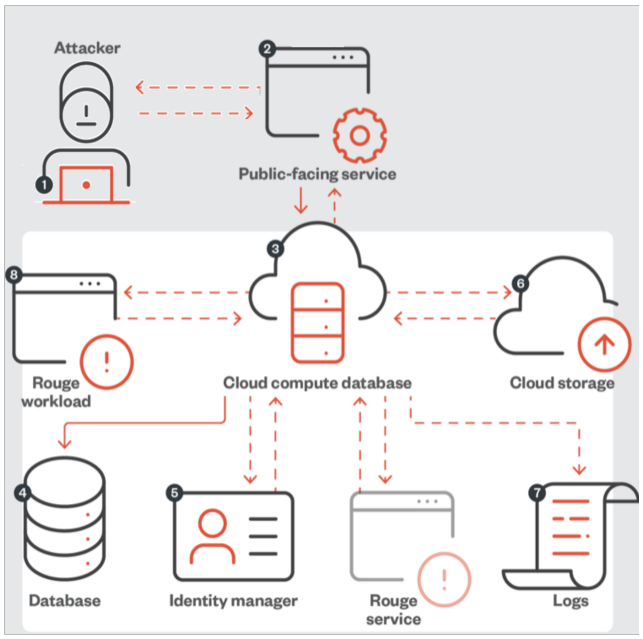

Fig 3. Privilege escalation within 5G cloud native

Authorized licensed use limited to: Indian Institute of Technology Hyderabad. Downloaded on May 27,2024 at 06:54:59 UTC from IEEE Xplore. Restrictions apply.

disable the ability to monitor actions made inside the compromised service.

B. Lateral movement for a data breach

An attacker could exploit a serverless application using the internal API system of the cloud service provider to check its permissions, see Fig. 4. When the serverless application has read and write permissions on its cloud storage services, the attacker could upload a command-line interface tool that not only allows the querying of the application's permission status but also the dumping or changing of cloud storage services.

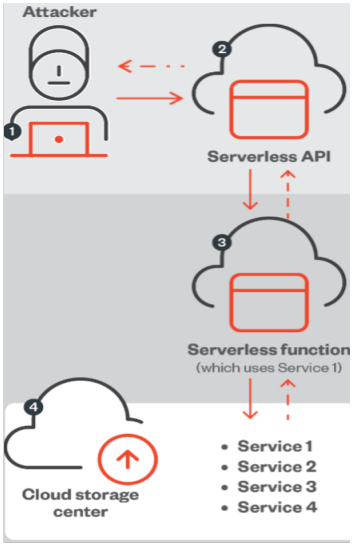

Fig 4. *Abusing a serverless application for lateral*

C. Vulnerabilities with Access Control Systems

The conventional access control systems can regulate access to resources by known users but are inadequate for open and decentralized multi-centric systems such as 5G native cloud where the user population is dynamic, and identity of all users are not known in advance. [5, 6] There are a lot of different 'hands in the bucket' because service providers and other third-party companies maintain and operate on these cloud servers. The organization will not know everyone working with their system beforehand. It will also be irrational and redundant if the organization assigns roles to these third-party engineers for their systems. Authors in [1] proposed a credential-based access control to satisfy the cloud's anonymity and dynamic resources. This access control is when a user's credentials are used to define access control policy, and anyone who possesses desired credentials is granted access to the shared data resource. User acquires the required set of credentials and submits it along with the data access request [1]. This type of access control can assist with the distributed environment because users are issued different credentials based on what they need to access. The user's credentials are verified through the CBAC system when accessing the entity, which is how they gain access to what they need, see Fig. 5. However, credentials can be compromised, and everyone involved will need to be registered in the system. Thus, we have to bring the zero trust security principles to the cloud environment to keep information secure so that we can attempt to promote perfect forward secrecy, where one attack on a user's credentials does not allow an attacker into the internal network. When implemented into 5G native cloud environment, a change in access control is needed.

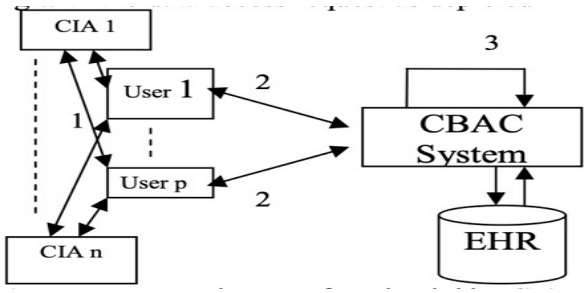

Fig 5. Credential-Based Access Control process [1]

Another interesting research that integrates the zero trust and access control models is the network simulation work presented in [4]. The authors created a hundred random sensor nodes, including genuine (which behave well) and malicious (which create attacks and DoS). Their first simulation was to see if a node with high centrality degree leads to a higher risk degree, and they were correct. In Fig. 6, we can see that when there are no malicious nodes and the centrality degree is 0, signifying they don't have neighbors, there are no attacks. However, when malicious nodes are present, and the centrality degree is 10 or 5, the network suffers degradation." This leads to the conclusion that "malicious nodes with more neighbors will indeed cause greater damage to the network [4].

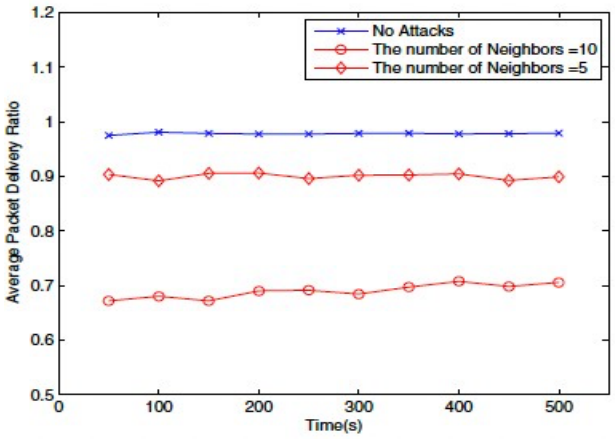

Fig. 6. Effect of High Centrality Degree of a Node [4]

III. Zero Trust and Access Control Data Breaches

The integration of zero trust principles to the access control model will assist with user manipulation, poor security, and misconfigurations in the network. Fig. 7 depicts that within last 20 years, there have been more than 150 variant data breaches caused by lost devices, stolen credentials/devices, poor security, accidentally published, misconfiguration of the network, and insiders exposing essential information [3].

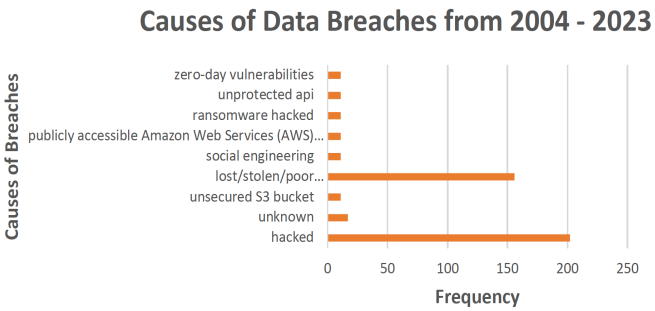

Fig 7. Causes of Data Breaches from 2004 – 2023 [3]

Because of lost and stolen devices, this paper implements the strip of the trust signature and user behavior (i.e., device

Authorized licensed use limited to: Indian Institute of Technology Hyderabad. Downloaded on May 27,2024 at 06:54:59 UTC from IEEE Xplore. Restrictions apply.

location). The system can no longer trust someone using a new device because it is unknown in the network and can no longer trust someone with two vastly different location sign-ins. For example, a user signing in from New York and then signing in from Florida an hour later is impossible. A properly developed ZTA should prevent a compromised account or asset from accessing resources outside its normal purview or access patterns. This means that accounts with access policies around resources that an attacker is interested in would be the primary targets for attackers, not just any user with access to the network [1]. Poor security, accidentally published information, and insiders exposing information are all part of access control and risk management. Risk management monitors the actions within the network and can work with access control to change a user's permissions in a live session. Fig. 8 depicts the three key factors that impact the risk management namely (1) the continuous multi-factor authentication indicating a constant continuation of user monitoring and authentication. (2) audits help in finding and assessing the vulnerabilities existing within the 5G cloud native networks and connected devices and measures to protect assets and minimize the possibility of fraud. (3) Intrusion Detection System (IDS) security alerts provide severity level of each related security events.

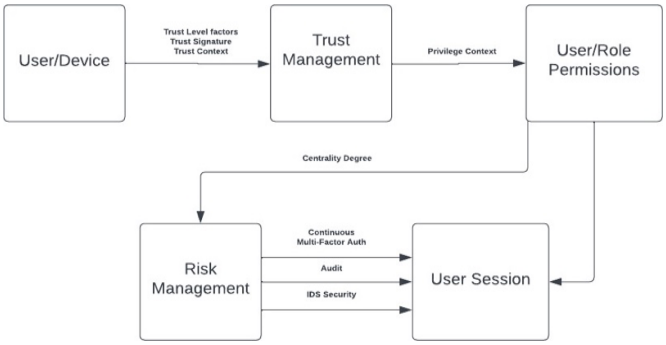

Fig 8. Zero Trust and Access Control Model Flow Chart

IV. PROPOSED CONTRIBUTIONS

A. *Trust within the Access Control Systems*

To have a secure access control system in the cloud environment, we must find a way to trust users/devices. The Zero Trust model says to "never trust, always verify". The organization has to find a way to create relationships between its system and users so that information can be accessed. They will also have to constantly verify that the user is whom they say they are, but this begins with how trust is viewed.

Trust is the firm belief in the competence of an entity to act dependably and securely within a specific context [6]. For a system to give access to a user, there has to be some confidence and relationship between the company and the user. We know that the company cannot trust the user entirely because of insider threat risk, so two different trust evaluations: Direct trust and Indirect trust evaluations.

- **Direct:** This trust contains the factors that involve the user directly. This includes their identity and their behavior history. The factors of this trust evaluation are also weighed more than the Indirect trust.
- **Indirect:** This trust evaluation contains the factors from second-hand users. This includes recommendations for the user and the user's experience interacting with the system.

The factors for each trust evaluation are:

- **Identity (Direct Trust)**: This is the first authentication step in traditional access control models, and users must provide credentials to access any resources. Users must be able to sign in with their organization's username and password to access organizational files. In this model, users are able to provide proof of identity/credentials to the organization and "exchange it with trust and access resources using trust" [5].
- **Behavior history (Direct Trust)**: The user's behavior is monitored. It can check if the user is accessing files for job duties, trying to access files they are not supposed to, the location the person is logging into their account from, or seeking information/files for things that do not pertain to their job. "At the start, the default historical access trust is zero, and the user gradually earns his historical access trust" [5].
- **Recommendation (Indirect Trust)**: The system will gather and evaluate recommendations sent from other users that pertain to the user in question.
- **Experience (Indirect Trust)**: The user's experience with the number of times they interact counts towards their trust level.

These factors are essential because the systems have to make sure that users abide by the policies that are put in place by the organization. This also creates a trusting relationship between the user and the org. These factors will have different weights depending on the truster (domain). The organization has to know which factor is more essential than the other and proceed with implementing the corresponding weight; the more influential the factor is, the higher the weight. For example, the user's behavior history would have a higher weight than the other factors because we can use or retrieve the behavior history data from the organization's insider threat detection system. This data will answer if a user can be trusted and what trust level they can receive. Because we want this also to be a dynamic access control system, we want to allow the results of these factors to change. Good recommendations, behavior, and more experience will increase the results, and the domain will have a higher chance of trusting the user. When the user's behavior begins to change and becomes suspicious, the trust level begins to decrease.

We can implement this trust model as an extension of the RBAC (Role-Based Access Control) model. This model T-RBAC will hold the same elements and sets that the RBAC model contains: *user, user_properties, session_instance, session_type, session, session_history, role, object, action, permissions, constraints* plus the *trust_level, privilege_context, trust_context, and trust_signature* element and set.

- *Trust_level*: Combines all the factors listed above and outputs a number between [0,5].
- *Privilege_context*: A checklist that users need to fulfill to have privileges to a role.
- *Trust_context*: Incorporates the trust evaluation to output whether a person is trustworthy.
- *Trust_signature*: Labels that identify the combination of trust level and trust context.

Authorized licensed use limited to: Indian Institute of Technology Hyderabad. Downloaded on May 27,2024 at 06:54:59 UTC from IEEE Xplore. Restrictions apply.

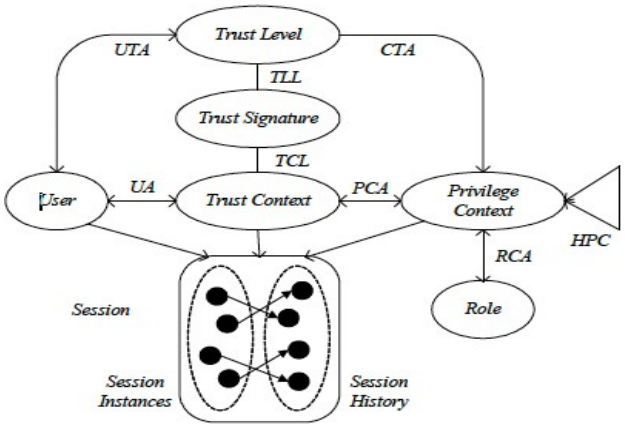

Fig 9. Trust combined with the Role-Based Access Control Model [1]

In Fig. 9, we can see how all of the elements that are incorporated in this model work. The Trust Context receives the user's trust factors and does a trust evaluation on them. Based on that trust evaluation, the user receives a trust level as well as a trusted signature (label) of how much they can be trusted. This is all presented in a privileged context. Each role has a checklist that needs to be fulfilled for a user to have access to the role. The privileged context takes the checklist for the role and the trust evaluation information and connects a user to the role through the session. The trust evaluation is the most important here because if the trust level changes, the trust signature and context change, which will most likely revoke access to a role or to specific files [7]. Implementing trust into access control models is supposed to take anonymity, unpredictability and uncertainty under control and assist decision arising from access from distinct domains [8]. Every device or user attempting to connect to the system and access files is assigned a trust context based on the different trust factors and credentials. Even though not everyone that accesses the system is known, they are assigned a trust context, and with that, their access can be restricted. This allows administrators to keep their systems under control and secure from anonymity and unexpected attacks.

B. Risk within the Access Control Systems

In this specific proposal, we want to include risk as another aspect to decide on user access. Even though we need to know a user's trust value to evaluate their risk, they represent different aspects when implemented into the Access Control model. As mentioned, trust focuses on not trusting every user who tries to access the system but assigning them a label based on their experience. Trust is used to indicate the extent to which subjects of accesses can be trusted [8]. The risk aspect of this Access Control model focuses on evaluating the user based on their trustworthiness. Risk is the prerequisite of trust. If there is no risk involved, there is no need to trust. The amount of trust required seems to depend on the risk involved [8]. The definition of risk is the possibility of being negatively impacted by a decision or action. In a distributed environment, risk is as important as trust. Administrators need to make sure that users within the system do not have the privilege to leak company assets/intellectual property. Risk can be calculated using the centrality degree.

Centrality Degree is originally used in networks to calculate the number of edges a node has. It is used to analyze the relations between one person and other entities (neighbors). An access control system environment can be used to see a user/node's popularity. For example, users with a higher centrality degree indicate that they attract more attention than other users [8]. This can also be how much a user is involved within the company. A company can have a Senior Administrator that has access to many assets of the company, so in this case, this user will need to have a high centrality degree. For this access control system, we will use this centrality degree to take part in the evaluation of risk. This degree can be ranked by who is more involved with the 5G cloud native network and the number of files someone can access.

C. Trust evaluation and Role-Based Access Control Scenarios

In this section, we will give various scenarios on the process of a device, whether it's known in the network or not. We will use the trust factors as well as the elements listed above and evaluate them based on how to gain access to the network and the permissions attached to their roles embedded in the system.

Scenario 1: A known user logs into the 5G system with an unknown device.

- The system will make sure that the user is not logged into their network account with multiple devices. If they are, it will automatically sign out the device the user previously signed in with. The more devices a user is logged into, the more it will affect their behavior trust factor.
- The system will then begin to evaluate the user's trust level.
  - Identity: Did the user successfully login?
  - Behavior History: Does our IDS (insider detection system) make the user seem suspicious? Is there any unusual behavior? Where are they logging in from? What was their location from last login?
  - Recommendation: Can anyone vouch for the user?
  - Experience: Is the user new? Is the device new?
- Based on the output of the trust level, the system gets the trust context.
- The trust signature is removed because the device is unknown to the system.
- Then, based on the user and their role, the system checks their permissions/privileges in the network (files that can be accessed).
- We will also use tools from the Zero Trust Architecture like Continuous Multi-factor Authentication so that the user is constantly authenticating themselves and the 5G cloud native network makes sure the user is who they say they are.
- As time goes by and the system determines this device is not a high risk anymore, it attaches the trust signature to it.

Scenario 2: An unknown user logs into the network's system with an unknown device.

- The only way an unknown user will be able to access the network is to have newly created account credentials, which will be set up by the 5G service operator.
- The user starts at the lowest trust level (1) because they

Authorized licensed use limited to: Indian Institute of Technology Hyderabad. Downloaded on May 27,2024 at 06:54:59 UTC from IEEE Xplore. Restrictions apply.

do not have experience with the system. If they are a vendor who sets up the virtual network, then they will have recommendations. This is all inputted while the account is set up.

- The user will not have permission or access to anything unless it is requested.

Scenario 3: A known user logs into the 5G network with a known device.

- The system will make sure that the user is not logged into their account using another device.
- The system will evaluate the user's trust level from their previous session. If nothing is suspicious, the user proceeds to log in and access their files.

While these scenarios seem redundant, they are not. Administrators need to have the mindset that all users, unknown and known, are vulnerabilities to the network. There has to be Zero Trust within the network to keep essential information secure. Implementing these trust factors and access control elements to the role-based access control model allows users to be more careful in what they are accessing and how they are accessing objects.

V. Simulations and Results

We conducted an experiment by using a mixed dataset extracted from two datasets that we created in our lab. The first dataset is a 5G user equipment biometric based data that contains identity scores for genuine and imposter users. Using this dataset, we determined the FAR (false acceptance rate) and FRR (false rejection rate) compared to a database with the facial recognition system. The other dataset contains behavior scores based on the 5G user equipment used in the mental health domain. We extracted the behavior scores from this dataset. We took the identity and behavior scores columns and fused both columns together. We also randomly inputted scores to the experience and recommendation scores to find out how a trust level should be outputted. Therefore, in our mixed dataset, we have identity scores, behavior scores, recommendation scores, and experience scores. We used Eq. 1 for computing a reasonable trust level score:

$$Trust\ level = !(Identity\ Score) * 0.44 + !(Behavior\ Score) * 0.34 + !(Recommendation\ Score) * 0.24 + ((Experience\ Score) * 0.1) \quad (1)$$

These scores are calculated based on the number of times a user access the network. Every time a user tries to access the 5G native cloud network, an identity score is recorded.

Identification Score: Calculated using multiple factors: the number of different locations a user tried to access the network from, the number of devices a user uses to access the network, and the number of times they fail to enter the correct password. We use the summation of these different factors and divide it by the number of times they try to log in.

Behavior Score: This score measures the user relative to all other users. This score can come from trusted third-party software used to detect anomaly behavior. Behavior detection software will determine whether the user is consistent in how they access our 5G cloud native network assets.

Recommendation & Experience Score: These scores will most likely be manual input from an administrator. The recommendation score will determine whether the user is known and trusted. The experience score can be a score that increases automatically based on the period (in days and weeks) the user is associated with the network.

This will determine the user's familiarity with the network's security policies and the steps to securing a highly sensitive environment.

In Fig. 10, the decimals (0.4, 0.3, 0.2, and 0.1) are weights. These weights are set by the 5G operator depending on what they would like to focus on more. For this first formula, we focused more on direct trust (identity and behavior) than indirect trust (recommendation and experience). The identity score containing a weight of 0.4 reflects the importance of verifying the user's identity. Users cannot access any resources within the company's domain without credentials. The behavior score being 0.3 reflects the user's past behavior. The lower the behavior score, the less trust the system will have in the user because they are indulging in suspicious activity. The recommendation score is assigned 0.2 because feedback from other users can be useful information, and lastly, the Experience score is assigned 0.1 to reflect their familiarity with the 5G operator's network and security practices.

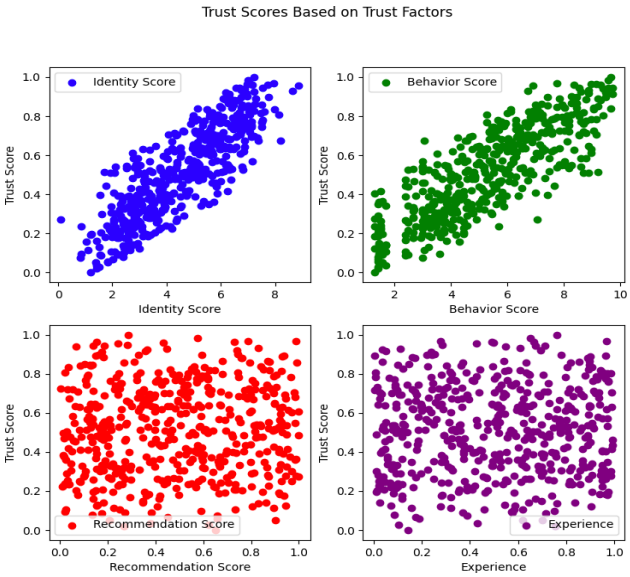

Fig 10. Impact from Categories to Trust level

Fig. 11 shows the impact that each category has on the trust score. We can see that the identity and behavior scores seem linear with the Trust score, meaning they have a stronger impact on whether a user will be accepted into the system as a trustworthy subject. Recommendation and Experience scores are useful information about a subject but don't have much of a say in this situation. In Fig. 11, we used Scikit-learn Logistic Regression to bring the data together and indicate whether the users were trustworthy. Based on the users in the dataset, we can see that most of them are trustworthy. If we look back at Fig. 10, we can see that there are more scores closer to 1. The higher the score of the trust factors, the higher the trust level will be and the more likely the system will allow the users access to its resources.

Authorized licensed use limited to: Indian Institute of Technology Hyderabad. Downloaded on May 27,2024 at 06:54:59 UTC from IEEE Xplore. Restrictions apply.

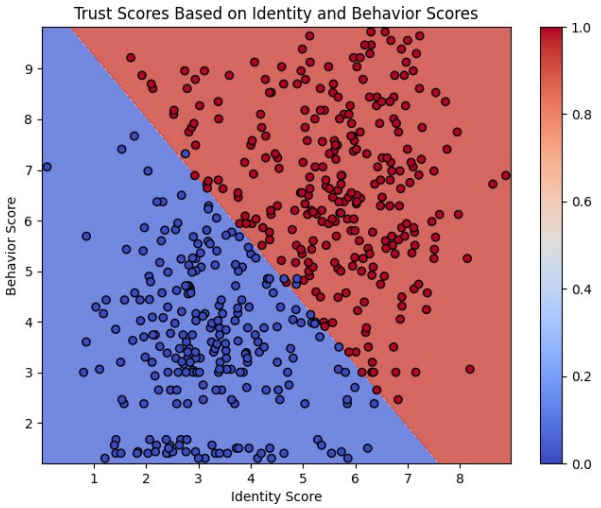

Fig 11. Determining the trustworthiness based on the Trust factor categories

In Figure 12, we can see a scatter plot of the experience and Recommendation scores together. We can deduce that this plot has no correlation, meaning that experience and recommendation alone will not enable a user's access to a resource. For example, in a 5G network, users with long term contracts/SLA are always considered first for valued benefits. In this case, one can see that other recommendation factors rather than long term SLA may not play a role in trustworthiness. Based on the color palette in Fig. 12, the darker color means the user is possibly not a trustworthy person within the network. Most users in this experiment with a high recommendation have a darker blue. This can relate to the risk the user has. As we mentioned, a user with high centrality degree can possibly be a high risk to the network's assets. They can attract a lot of attacker attention.

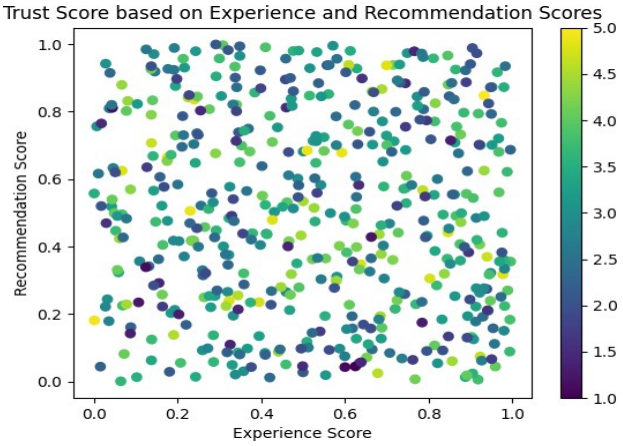

Fig 12. Correlation between Experience and Recommendation Scores based on Trust Score

In Fig. 13, we decided to change the weights for Eq. 1 by relying more on the behavior score than the identity score. We set the identity's score weight to 0.3, and the behavior's score to 0.4. Thus, the number of trustworthy users decreases since the trust equation penalizes the users with low behavior scores indicating they are conducting more unusual activity than other users. Again, the 5G operators implementing this ZT system can change the weights for each factor based on what they prefer is essential to access their sensitive assets.

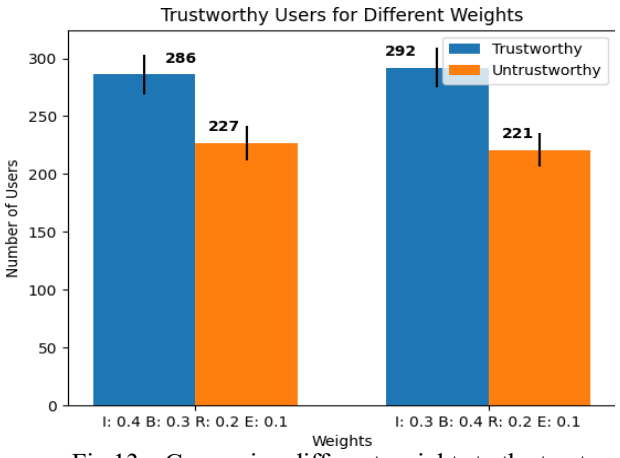

Fig 13. Comparing different weights to the trust evaluation formula

VI. Conclusion

An access control model is able to keep the integrity of organizational assets in-house. When other factors come into play, like the move of an on-premises system to 5G cloud native systems, access control becomes volatile. Implementing a zero-trust architecture with access control is essential. Trust and Risk provide zero trust in any access control model. Trust is able to protect the organization's network and files from unknown devices and users. Risk provides dynamic change within the access control as well as constant authentication for the user depending on their trust level. We proposed zero trust model that combines the principles of access control systems and the trust evaluation by factoring in the user's behavior, identity, and recommendations.

For future work, we plan to extend our current cybersecurity framework [9-43] with the zero trust and access control features discussed in this paper.

VII. Acknowledgment:

This research was supported in part by the Air Force Research Laboratory through the Information Directorate's Information Institute® contracts numbers FA8750-23-C-0517 and SA10032023050659".

VIII. References

[1] Chakraborty S., Ray, I. "TrustBAC – Integrating Trust Relationships into the RBAC Model for Access Control in Open Systems". 2006. Colorado State University.

[2] Dagdee, Dr. N., Ruchi, V. "Access control methodology for sharing of open and domain confined data using Standard Credentials." November 2009. International Journal on Computer Science and Engineering.

[3] Data Breaches. https://www.kaggle.com/datasets/thedevastator/data-breaches-a- comprehensive-list

[4] Duan, J., Deyun, G., Foh, C. H., Leung, V. "Trust and Risk Assessment Approach for Access Control in Wireless Sensor Networks" 2013.

[5] Helil, N., Kim, M., Han, S. "Trust and Risk-based Access Control and Access Control Constraints". November 2011. KSII Transactions on Internet and Information Systems Vol. 5, No. 1.

[6] Li, Y., Sun, H., Chen, Z. "Using Trust and Risk in Access Control for Grid Environment". 2008. IEEE Xplore.

[7] Rose, S., Borchert, O., Mitchell, S., Connelly, S. "NIST Special Publication 800-207 Zero Trust Architecture" NIST. August 2020.

[8] Yang, R., Lin, C., Jiang, Y., Chu, X. "Trust Based Access Control in Infrastructure- centric Environment". IEEE ICC, 2011

Authorized licensed use limited to: Indian Institute of Technology Hyderabad. Downloaded on May 27,2024 at 06:54:59 UTC from IEEE Xplore. Restrictions apply.

[9] Badr, Mahmoud M., Mohamed I. Ibrahem, Hisham A. Kholidy, Mostafa M. Fouda, and Muhammad Ismail. 2023. "Review of the Data-Driven Methods for Electricity Fraud Detection in Smart Metering Systems" Energies 16, no. 6: 2852. https://doi.org/10.3390/en16062852

[10] A. H. M. Jakaria, Hisham A. Kholidy, et al., "Trajectory Synthesis for a UAV Swarm Based on Resilient Data Collection Objectives," in IEEE Transactions on Network and Service Management, vol. 20, no. 1, pp. 138-151, March 2023, doi: 10.1109/TNSM.2022.3216804.

[11] Hisham A. Kholidy et al., "Toward Zero Trust Security IN 5G Open Architecture Network Slices," MILCOM 2022 - 2022 IEEE Military Communications Conference (MILCOM), Rockville, MD, USA, 2022, pp. 577-582, doi: 10.1109/MILCOM55135.2022.10017474.

[12] Hisham A. Kholidy and S. Hariri, "Toward An Experimental Federated 6G Testbed: A Federated Leaning Approach," 2022 IEEE/ACS 19th International Conference on Computer Systems and Applications (AICCSA), Abu Dhabi, United Arab Emirates, 2022, pp. 1-6.

[13] Hisham A. Kholidy, A. Karam, J. H. Reed and Y. Elazzazi, "An Experimental 5G Testbed for Secure Network Slicing Evaluation," 2022 IEEE Future Networks World Forum (FNWF), Montreal, QC, Canada, 2022, pp. 131-138, doi: 10.1109/FNWF55208.2022.00032.

[14] Hisham A. Kholidy, "Multi-Layer Attack Graph Analysis in the 5G Edge Network Using a Dynamic Hexagonal Fuzzy Method", Sensors 2022, 22, 9.

[15] Hisham A. Kholidy, A. Karam, J. L. Sidoran, M. A. Rahman, "5G Core Security in Edge Networks: A Vulnerability Assessment Approach", the 26th IEEE Symposium on Computers and Communications, Greece, September 5-8, 2021.

[16] Hisham A. Kholidy, "A Triangular Fuzzy based Multicriteria Decision Making Approach for Assessing Security Risks in 5G Networks", December 2021, {2112.13072}, arXiv.

[17] Hisham A. Kholidy, Fabrizio Baiardi, "CIDS: A framework for Intrusion Detection in Cloud Systems", in the 9th Int. Conf. on Information Technology: New Generations ITNG 2012, April 16-18, Las Vegas, Nevada, USA. http://www.di.unipi.it/~hkholidy/projects/cids/.

[18] Kholidy, H.A. (2020), "Autonomous mitigation of cyber risks in the Cyber–Physical Systems", Future Generation Computer Systems,Volume 115, 2021, Pages 171-187, ISSN 0167-739X, https://doi.org/10.1016/j.future.2020.09.002.

[19] Hisham A. Kholidy, Abdelkarim Erradi, Sherif Abdelwahed, Fabrizio Baiardi, "A risk mitigation approach for autonomous cloud intrusion response system", Computing Journal, Springer, June 2016. (Impact factor: 2.220). https://link.springer.com/article/10.1007/s00607-016-0495-8

[20] Hisham A. Kholidy, "Detecting impersonation attacks in cloud computing environments using a centric user profiling approach", Future Generation Computer Systems, Vol 115, 17, December 13, 2020, ISSN 0167-739X.

[21] Hisham A. Kholidy, Baiardi, F., Hariri, S., et al.: "A hierarchical cloud intrusion detection system: design and evaluation", Int. J. Cloud Comput., Serv. Archit., 2012, 2, pp. 1–24.

[22] Hisham A. Kholidy, "Detecting impersonation attacks in cloud computing environments using a centric user profiling approach", Future Generation Computer Systems, Volume 115, issue 17, December 13, 2020, Pages 171-187, ISSN 0167-739X.

[23] Hisham A. Kholidy, "Correlation-based sequence alignment models for detecting masquerades in cloud computing", IET Information Security, 2020, 14, (1), p.39-50.

[24] Hisham A. Kholidy, Abdelkarim Erradi, "A Cost-Aware Model for Risk Mitigation in Cloud Computing SystemsSuccessful accepted in 12th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA), Marrakech, Morocco, November, 2015.

[25] Hisham A. Kholidy, Ali T., Stefano I., et al, "Attacks Detection in SCADA Systems Using an Improved Non-Nested Generalized Exemplars Algorithm", the 12th IEEE Int. Conference on Computer Engineering and Systems, December 19-20, 2017.

[26] Qian Chen, Hisham A. Kholidy, Sherif Abdelwahed, John Hamilton, "Towards Realizing a Distributed Event and Intrusion Detection System", the Int. Conf. on Future Network Systems and Security, Florida, USA, Aug 2017.

[27] Hisham A. Kholidy, A. Erradi, Sherif Abdelwahed, Abdulrahman Azab, "A Finite State Hidden Markov Model for Predicting Multistage Attacks in Cloud Systems", in the 12th IEEE Int. Conf. on Dependable, Autonomic and Secure Computing, China, August 2014.

[28] Ferrucci, R., & Hisham A. Kholidy (2020, May). A Wireless Intrusion Detection for the Next Generation (5G) Networks", Master's Thesis, SUNY poly. 33. Rahman, A., Mahmud, M., Iqbal, T., Saraireh, L.,

[29] A.-u. Rahman, M. Mahmud, T. Iqbal, L. Saraireh, Hisham A. Kholidy, M. Gol-lapalli, D. Musleh, F. Alhaidari, D. Almoqbil, and M. I. B. Ahmed, "Network anomaly detection in 5g networks." Mathematical Modelling of Engineering Problems, vol. 9, no. 2, 2022., pp. 397-404. https://doi.org/10.18280/mmep.090213.

[30] Hisham A. Kholidy, "An Intelligent Swarm based Prediction Approach for Predicting Cloud Computing User Resource Needs", the Computer Communications Journal, December 2019.

[31] Hisham A. Kholidy, "Towards A Scalable Symmetric Key Cryptographic Scheme: Performance Evaluation and Security Analysis", IEEE Int. Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, May 1-3, 2019.

[32] Samar SH. Haytamy, Hisham A. Kholidy, Fatma A. Omara, "Integrated Cloud Services Dataset", Lecture Note in Computer Science, ISBN 978-3-319-94471-5, https://doi.org/10.1007/978-3-319-94472-2. 14th World Congress on Services, 18-30. Held as Part of the Services Conf. Federation, SCF 2018, Seattle, WA, USA.

[33] Hisham A. Kholidy, Ali T., Stefano I., Shamik S., Qian C., Sherif A., John H., "Attacks Detection in SCADA Systems Using an Improved Non- Nested Generalized Exemplars Algorithm", the 12th IEEE Int. Conf. on Computer Engineering and Systems (ICCES 2017), Feb. 2018.

[34] Hisham A. Kholidy, F. Baiardi, "CIDD: A Cloud Intrusion Detection Dataset for Cloud Computing and Masquerade Attacks," 2012 Ninth Int. Conference on Information Technology - New Generations, 2012, pp. 397-402, doi: 10.1109/ITNG.2012.97. 39. Differentially Private Stochastic Gradient Descent. https://medium.com/pytorch/differential-privacy-series-part-1-dp-sgd-algorithmexplained-12512c3959a3

[35] M. Alkhowaiter, H. Kholidy, M. A. Alyami, A. Alghamdi, and C. Zou, "Adversarial-aware deep learning system based on a secondary classical machine learning verification approach," Sensors, vol. 23, no. 14, p. 6287, 2023.

[36] F. M. Mustafa, H. A. Kholidy, A. F. Sayed, M. H. Aly, and F. Elmisery, "Backward pumped distributed raman amplifier: enhanced gain," Optical and Quantum Electronics, vol. 55, no. 9, p. 772, 2023.

[37] T. J. Alahmadi, A. U. Rahman, H. K. Alkahtani, and H. Kholidy, "Enhancing object detection for vips using yolov4 resnet101 and text-to-speech conversion model," Multimodal Technologies and Interaction, vol. 7, no. 8, p. 77, 2023.

[38] M. C. Zouzou, E. Benkhelifa, H. Kholidy and D. W. Dyke, "Multi-Context-aware Trust Management framework in Social Internet of Things (MCTM-SIoT)," *2023 International Conference on Intelligent Computing, Communication, Networking and Services (ICCNS)*, Valencia, Spain, 2023, pp. 99-104, doi: 10.1109/ICCNS58795.2023.10193510.

[39] I. Elgarhy, M. M. Badr, M. Mahmoud, M. M. Fouda, M. Alsabaan and Hisham A. Kholidy, "Clustering and Ensemble Based Approach For Securing Electricity Theft Detectors Against Evasion Attacks", in IEEE Access, January 2023, doi: 10.1109/ACCESS.2023.3318111. (IF: 3.55).

[40] Alkhowaiter, M.; Hisham A. Kholid.; Alyami, M.A.; Alghamdi, A.; Zou, C, "Adversarial-Aware Deep Learning System Based on a Secondary Classical Machine Learning Verification Approach". Sensors 2023, 23, 6287. https://doi.org/10.3390/s23146287 (IF: 3.9).

[41] Robert Bohn, Abdella Battou, Baek-Young Choi, Ranganai Chaparadza, Sejun Song, Tao Zhang, Taesang Choi, Hisham A. Kholidy, Moonkook Park, SeungKyu Go, "NIST Multi-Domain Knowledge Planes for Service Federation for 5G & Beyond Public Working Group: Applications to Federated Autonomic/Autonomous Networking", accepted and to be appeared in the IEEE Future Networks World Forum (FNWF), 13–15 November 2023 // Baltimore, MD, USA.

[42] M. C. Zouzou, E. Benkhelifa, Hisham A. Kholidy and D. W. Dyke, "Multi-Context-aware Trust Management framework in Social Internet of Things (MCTM-SIoT)," 2023 International Conference on Intelligent Computing, Communication, Networking and Services (ICCNS), Valencia, Spain, 2023, pp. 99-104, doi: 10.1109/ICCNS58795.2023.10193510.

[43] Malkoc, M., & Kholidy, H. A. (2023). 5G Network Slicing: Analysis of Multiple Machine Learning Classifiers. ArXiv. /abs/2310.01747

Authorized licensed use limited to: Indian Institute of Technology Hyderabad. Downloaded on May 27,2024 at 06:54:59 UTC from IEEE Xplore. Restrictions apply.